ARE YOU WHO YOU SAY YOU ARE? COMPUTER SCIENCE AND THE PROBLEM OF DIVINE SELF-AUTHENTICATION

by Andrew McFarlane

Abstract. A vital axiom of Reformed theology is that God is who God claims to be, and that he acts to "self-authenticate" his identity to humans through the internal witness of the Holy Spirit. But how ought theologians to represent and make sense of the multiform nature of divine self-authentication (DSA)? And can their models account for the various kinds of evidence God utilizes in acts of DSA, or explain why doubt and deception about divine identity persists despite it? Operating at the intersection of theology and computer science, this study examines how modern authentication technologies can deepen theological reflection upon the nature, evidence, and efficacy of DSA. It proposes that computer authentication "trust systems": (1) offer a valuable schematic for representing the variegated structural patterns inherent in DSA; (2) shed critical light on the forms and functions of evidence used in DSA; and (3) provide strategies and practical measures for offsetting the continuing risk of deception about human and divine identity.

Keywords: authentication; computer science; divine action; evidence; identity; reformed theology; religious belief; trust

Introduction

The use of authentication methods to discern who should be trusted is a long-established human practice which facilitates security, surveillance, and access control to protected places and information (Smith 2002, 5). In Christian theology, too, authentication is an axiomatic epistemological concept. The idea that God genuinely is who God reveals himself to be in the Bible, and is not an imposter, is the acknowledged basis of church life and doctrine (Barth 1957, 204). A related thesis of Reformed theology is that God's identity claims are trustworthy because divine action is "self-authenticating," that is, possesses and communicates its own "intrinsic credibility" independently of human judgment and

Andrew McFarlane is a manager of Enterprise Data Services at the University of Edinburgh, UK; e-mail: andrew.mcfarlane@ed.ac.uk.

 ISSN 0591-2385

human-produced evidence (Wahlberg 2020). For key Reformed thinkers such as John Calvin, Karl Barth, and Thomas Torrance, the activity of divine self-authentication (hereafter "DSA") is a Trinitarian event spearheaded by the Holy Spirit who testifies to God's identity and intentions through a range of divinely authorized witnesses including the Bible, miracles, conscience, and more.

While Reformed theology upholds what Calvin called the "internal witness of the Holy Spirit" as a cornerstone of theological epistemology, there are surprisingly few studies of *how* the Spirit authenticates divine identity to humans. Past and present accounts of the Spirit's work of assurance focus upon its biblical basis, its epistemically anchoring role in the Christian life, and upon the miraculous nature of the religious experience that purportedly attends it (Pelikan 1989, 162–74). Yet there is little information available about what happens operationally on the "divine-side," as it were, when God executes an act of DSA. So how ought theologians to make sense of and represent this complex, multiform class of divine action? This article proposes an answer leveraging the insights of computer science, a mathematical discipline widely credited with having pioneered modern authentication theory and practice. It contends that computer authentication "trust systems"—a select network of entities and mechanisms which dynamically cooperate on command to verify an identity claim—can usefully function as a rough image, or what Kallenberg terms a "disclosure model," for representing the complex, multiform nature of DSA (Kallenberg 2015, 34–35).

Beyond that contention, this study proposes two further contributions computer science makes to the Reformed understanding of DSA. First, computer science provides a fresh angle from which to think about the evidence the Bible says God uses to support human belief in his identity claims. The forms and functions of evidence in computer authentication are shown to offer a useful platform for reflecting upon the question of what counts as evidence of divine identity, and for highlighting the importance of the temporary and often single-use character of such evidence. Second, computer science has much to say about why authentication sometimes fails, and about what can be done to minimize the risk of doubt and deception about identity. Acknowledging that acts of DSA are not always and everywhere successful—partly due to the work of malovent agencies—this study examines whether theology could reduce the continuing risk of deception about divine identity using principles and practices broadly informed by computer science.

Taken altogether, then, the proposal of this article is simply that by integrating the contributions of computer science on authentication systems, researchers can avail themselves of an expanded conceptual toolkit for better exploring and articulating the *nature*, *evidence*, and *efficacy* of DSA.

A key driver for bringing these admittedly very different disciplines together is that authentication is a topic of shared importance. Theology and computer science partner well on this topic because both are demonstrably invested in how to establish trusted identity and manage the potential for doubt and deception. For theology, the integrity of the knowledge of God—theology's core "knowledge bank"—depends on the assurance that God's identity is known and trustworthy. For computer science, there is an imperative to continually evolve authentication technologies to combat ever-increasing threats to the security of businesses, individuals, and governments. A core axiom of this study is therefore that, while markedly different disciplines, their approaches admit of contrast and comparison precisely because the assurance of correct identity is a task of shared interest and importance.

This article begins with a select overview of the authentication of identity in theology and computer science. First, theology: I introduce the appearance of DSA in early Reformed theology before considering what contemporary epistemological readings of the Bible reveal about its nature, evidence, and efficacy. As regards computer science, I outline the core concepts of human and computer authentication, including the idea of a trust system, and provide three commonplace and increasingly complex examples of such systems: username and password, biometrics, and public key infrastructure (PKI). With that groundwork complete, the remainder of this article unfolds how researchers can harness knowledge of computer authentication systems to shed light upon the nature, evidence, and efficacy of DSA.

This study approaches the concept of DSA from a broadly Reformed perspective. This means it treats DSA under the rubric of divine *self-revelation*, an idea regarded as central to the Reformed paradigm of epistemology (Torrance 2000). Within that paradigm, DSA comes to view as an operation of the Holy Spirit, and as such it is an activity whose redemptive function and meaning is anchored in the person and work of Jesus Christ, whose spirit it is. All pneumatologically-driven acts of DSA thus have Jesus Christ as their material, validating point of reference. Two broad types of DSA are distinguished. Type 1: a distinct class of revelatory divine acts whose primary purpose is to assure humans about divine identity (Calvin 1960; Moser 2017). Type 2: a property of assurance intrinsic to, and communicable by, all revelatory divine acts toward humans (Barth 1957; Torrance 1971). This article does not contest the validity and complementarity of these types, although it mainly targets Type 1 for analysis.

While this article treats the Reformed understanding of DSA, other theological traditions offer instructive approaches to divine authentication that for reasons of time and space cannot be explored here.[1] Furthermore, the word "assurance" is used throughout to signify the broad range

of outputs a successful act of DSA may produce within human experience, whether an intellectual conviction, religious experience, or a simple felt sense a believer may have that God really is who God claims to be. However, a taxonomy of assurance types and their undergirding warrants is not provided. This is because this article is focused upon the divine-side operational mechanics of DSA; questions concerning the human-side preconditions, reception, or results of DSA are of secondary concern.

Authentication of Divine Identity: Introducing DSA

Despite their varying epistemological assumptions and paradigms, almost all Christian traditions insist that God is somehow knowable. At stake in this claim is no less than the credibility of academic theology and the vitality of church life, since both rely on the assurance that knowledge of God is in some way available and can be trusted. But how do theologians come to certify as trustworthy the various sources of the knowledge of God—Bible, tradition, reason, and experience—not to mention the multitude of cognitive and noncognitive forms such knowledge may take? How is it established whether the God revealed and known through those sources is really who he claims to be?

One instructive line of reflection upon these questions is found in Reformed theology. There, the issue of how to authenticate the knowledge of God as genuine is a long-standing problematic emerging out of what Diller calls theology's "epistemological dilemma":

> It is a dilemma created by two competing assertions. The first affirms with confidence that theological knowledge – not mere theological *belief* – is a real human possibility. The second threatens that confidence with a recognition of human fallibility. Christian theology cannot dispense with its acknowledgement that we are humanly unable to self-secure the grounds of our theological knowledge, yet Christian theology must affirm that God makes himself humanly known. (Diller 2014, 295)

Although writing about Christian theology in general, Diller's dilemma is perhaps most acutely felt in the Reformed tradition, in which both its lemmas are deemed mainstream (if not universally held) views: (1) God is known and can be trusted, *but* (2) humans lack the tools to independently authenticate or validate the knowledge of God. Framed thus, this dilemma drives the question of authentication out into the open: if humans are unable to "self-secure" the knowledge of God for themselves, what grounds their belief that this knowledge is genuine and reliable?

A characteristic response within the Reformed tradition has been to claim that God *self-authenticates* himself to humans. To abstract from the complexities, this is a set of views which revolve around the idea that the grounds for human trust in divine identity claims rest only in God because it is God who personally authenticates himself, and the knowledge of

himself, in his self-communication through the joint operation of his Word (as heard in Scripture) and his Holy Spirit (Torrance 2000). While opinion varies about the types, forms, and applications of DSA—for example, is it a unique class of intentional divine acts or simply a dimension of all divine acts?—there is agreement about the broad purpose of DSA: God self-confirms his identity simply because it pleases him to provide humans with solid assurance of his identity and promises (Barth 1957, 12).

Within the history of Reformed theology, the idea of divine self-authentication (Gk. *Autopistia*) appears as a distinct concept in the work of Calvin, in his doctrine of the internal witness of the Holy Spirit. There, it is advanced to support the idea that the authority of Scripture derives, not from the consensus of the Catholic church, but from God alone (Calvin 1960, 1.7.5). While it is often assumed that by "self-authentication" Calvin meant that the text of the Bible somehow proves its own divine origin, this is not in fact what Calvin was proposing (van den Belt 2011). For Calvin, self-authentication is not a property of the Scriptures but is a *special divine act* which is specifically aimed at providing humans with an incontestable form of assurance that the Bible stands trustworthy as the authentic "voice of God." Through an act of DSA God authenticates the text to the believer. Humans come to perceive the genuine voice (or "Word") of God in the Scriptures through the hearing of faith which is effected by the testimony of the Holy Spirit. This testimony is "secret" and "internal" in as much as the Holy Spirit works *within* the human reader to authenticate the truth of Scripture in a supernatural moment of affective and cognitive confirmation (Calvin 1960, 1.7.4).

Thus described, DSA is an entirely spiritual event for Calvin in which human forms of evidence are given little epistemic load-bearing value. Solid proofs for the divine origin of Scripture can be summoned but Calvin considers them inferior to, and no substitute for, the Holy Spirit, whose witnessing work results in a "conviction that requires no reasons," "a feeling that can be born only of heavenly revelation" (Calvin 1960, 1.7.5). Authentic knowledge of God thus does not have its ground in human-produced evidence but, in Torrance's paraphrase of Calvin position, "emanates from a testimony inherent in God," that is, it flows from the Holy Spirit who, inhering in the truth of God's being, is God's own witness to himself. It is the conjoint action of Spirit and Word by which humans are brought to participate in this divine "self-knowledge and self-witness" (Torrance 2000).

Judging from its appearance in early Reformed dogmatics, it might seem that DSA is a concept which only finds distinct expression within debates about the authority of Scripture. However, there has been a recent resurgence of interest in DSA as a special divine act, with researchers extending theological understanding of it in several important directions. Experts in

church history have charted the concept's treatment within the history of Reformed dogmatics (van den Belt 2008), while scholars working in the area of "biblical epistemology" offer an account of DSA sourced directly from the Old and New Testament text (Healy and Parry 2007). Within contemporary philosophy of religion, too, argument abounds as to the role Calvin's classic account of DSA plays in the formation of warranted Christian belief (Plantinga 2000, 256).

The remainder of this section draws upon epistemological approaches to the Bible and outlines some of their observations regarding the nature, evidence, and efficacy of DSA.

In Moser's view, DSA in the Bible is a distinct class of divine self-demonstration (Moser 2017). Indeed, the Bible describes many occasions where God reportedly makes an identity claim about himself ("self-identification") and then acts specifically to confirm that claim ("self-authentication"). In the Old Testament, for instance, God self-identifies to Moses at the burning bush, not initially with a name, but by stating his relationship to the patriarchs, "I am the God of your father; the God of Abraham…Isaac…and Jacob" (Exodus 3:6 New Revised Standard Version (hereafter "NRSV")). This move is designed to assure Moses, for God identifies himself not as an unknown deity, but as one already personally known and trusted by Israel. By contrast, in the New Testament instances of divine self-identification are at a premium: Jesus is said to claim divine identity on numerous occasions, for example, when he uses the name "I am" for himself in John 8:58 NRSV.

There are several high-profile instances of divine self-authentication littered throughout the biblical narratives. At the pinnacle of Baal-worship in Israel, the Israelites knew who God claimed to be, but this was not sufficient to prevent their slide into idolatry. Elijah consequently calls on God to demonstrate who he is "so that this people will know that you, O Lord, are God" (1 Kings 18:37 NRSV). When God acts miraculously to burn up the sacrifice, this is accepted by the onlookers as evidence and proof of God's identity claim, "The Lord indeed is God!".

Turning to the New Testament, the Gospels describe several acts of DSA which center upon, or are carried out by, Jesus. At his baptism, for instance, the Holy Spirit descends from above to publicly authenticate Jesus' divine identity and messianic office, sealing the bond of love and trust between God the Father and God the Son. But it is the resurrection event that authenticates Jesus' own and earlier claim to the disciples that he is the "Son of Man" who "three days after being killed…will rise again" (Mark 9:31 NRSV). Postresurrection, Jesus attempts to confirm the truth of his identity by appearing to the incredulous, doubting disciples and telling them to "touch me and see" (Luke 24:39 NRSV). Not only did he authenticate himself to those he knew "by many convincing proofs" (Acts 1:3 NRSV), he attempted to convince many who did not know him.

After his ascension, Christ's work of self-witness continues up to the present day through the ongoing presence of his Spirit in the world. Throughout the Pauline corpus, the Holy Spirit is seen to witness to the truth of the resurrection to an ever-widening audience, using miracles and other means to cross-validate the Hebraic and Apostolic testimony to Christ the Messiah.

This small sampling is illustrative of a much wider testimony to acts of DSA seen within the Bible. From it, we can observe the following about the nature, evidence, and efficacy of DSA.

As regards the nature of DSA, it is apparent from the above that God may execute an act of DSA to confirm his existence and identity to those who do not know him (as per the New Testament miracle narratives) or use it to reassure or reconfirm some aspect of himself to those who already know him. Second, DSA takes different forms (i.e., utilizes a different range of spiritual and creaturely objects) depending on the context and purpose of its execution. Forms may include miracles, conscience, prophecy fulfilment, visions, dreams, and in the New Testament the spiritual formation of the Christian character (Moser 2017, 16). Third, when successful, acts of DSA often result in individual and communal transformation and repentance (Rae 2007, 174). DSA is seen to effect deepening trust in those who already know God. In those who do not, by contrast, it may instigate an event of faith—an event in which the human knowing of God takes place through the activity of the Holy Spirit, who links human hearing and divine speaking (Barth 1936, 238).

Intriguingly and importantly, however, the Spirit's work of authentication is not always efficacious. Doubt and deception about God's identity persist among God's people despite acts of DSA. A significant proportion of such acts *fail* owing to one of these two reasons:

i. The (in)sufficiency of evidence. The evidence used by God in his self-authentication seems to be needed for the act to be truly efficacious but is often shown to be insufficient of itself to always and everywhere establish human trust that God is who he claims to be. The Bible reports that such evidence is sometimes ignored, not recognized as evidence, is met with disbelief, or is simply not trusted. Consider Jesus' disciples who persist in confusion about his divinity despite having been party to several of his reported miracles—"What sort of man is this?" they ask each other in amazement after Jesus calms a storm (Matthew 8:27 NRSV). The Gospel of John also reports that many people allegedly witnessed Jesus' "signs" but that many "did not believe in him" (John 12:37 NRSV).

ii. Interference by malevolent human or spiritual agencies. The Bible notes numerous instances where doubt and deception about God's identity persists among God's people, despite God's work of self-demonstration and self-authentication, owing to interference from malevolent beings. Their aim is to diminish human trust in God's reality and identity by

intercepting and altering God's message or by undermining the human understanding of its received content. For example, Eve's confidence that God's word is trustworthy is undermined by the serpent, who successfully encourages her to doubt God's injunction not to eat from the tree of life (Genesis 3:1-8 NRSV). Malevolent spiritual agencies even attempt to impersonate God, such as in the case of Job, who is fooled into believing that the hardship that befalls him is from God when it is effected by Satan (Job 9:28-35 NRSV).

The Bible points to one root cause behind both these reasons for DSA failure: human "hardness of heart" or, otherwise put, a lack of "faith" (Moser 2017, 123). A degree of failure would therefore seem a logical byproduct of the program of salvation history. God knows and intends that not all will "look with their eyes" or "understand with their hearts" (John 12:40 NRSV).

Authentication of Human Identity: Computer Trust Systems

Turning now to the authentication of human identity, computer science is a mathematical discipline which has engineered many of the technologies of human authentication in widespread use today. It treats authentication as an aspect of computer security, a subfield concerned with the protection of IT resources from dangers and risks. A "resource" may be a system, the information it holds, the infrastructure it is built on, or the network that hosts it (Bishop 2003b). Protection is required from any potential or actual "violation of security" by which an agent could access, alter, or destroy a resource (Bishop 2003a, 6). Within the human sphere, authentication is thus first and foremostly a crucial *security measure* whose aim is to "ensure that entities are correctly identified" (Bishop 2003a, 311).

While computer-based authentication systems are complex and numerous, the basic principles that guide them are easy to grasp and have not changed much throughout history. The requirement to correctly identify people is age-old and stems from the perennial need to ensure that only allowed persons are granted access to high-value resources while those disallowed are kept out. People have always had to authenticate to others before being granted access to restricted areas, valuable items, or important people. For Samantha to enter the King's court, for example, it is not enough that she self-identify to the guard at the gate. She must also provide evidence that she is in fact the person she claims to be, perhaps by showing an identity document along with the official letter of summons she was sent. If the guard, on checking the evidence against the register of expected visitors, is satisfied that Samantha's identity claim is authentic then entry may be granted.

The purpose of human authentication—whether computerized or occurring as a physical, person-to-person interaction as in the example above—is simply to verify whether a person is who they say they are. Authentication methods aim to identify an unknown person who presents themselves for the first time, or reidentify someone already known. And it is not only persons who must authenticate; in the modern era devices such as computers and mobile phones are also required to confirm their identity to gain access to networks and online services and applications. The methods by which authentication happens each have differing levels of rigor and correspondingly different risk profiles. For instance, conducting an identity check via an informal person-to-person chat is an obviously more risk-laden method than computer authentication with its systems and formalized procedures. Yet despite their varying strengths and weaknesses, human authentication methods all exist upon a single continuum in virtue of a common feature, namely, their *claims-based* character. Human authentication methods cannot ontologically certify that Samantha really and truly is Samantha; they can only ever judge whether the visitor's *claim* to be Samantha is valid.

To perform its work, the practice of human authentication typically involves a set of agents and elements which work together as a system to judge whether an identity claim is correct. Such systems are termed *trust systems* because together their elements are directed toward establishing whether an identity declaration ought to be trusted. According to security expert Smith, computerized trust systems historically comprise these basic elements (Smith 2002, 3):

(1) *An identity claim*: a person who states an identity in order to access a resource

(2) *Supporting evidence*: a distinguishing characteristic, unique to a person, that can count as independent evidence of their stated identity

(3) *A judgment*: an objective means (a mechanism) for determining whether the evidence supplied is associated with the stated identity.

A key requirement of such trust systems is the availability of *supporting evidence*. Indeed, to minimize the potential for doubt and deception, authentication systems do not accept as valid a stand-alone identity claim. They will ask for corroborating evidence which will be checked to see if it validates the identity claimed.

Although views on what is considered acceptable evidence have varied markedly over the centuries, the guiding principle has remained the same: the submitted evidence ought to represent a distinguishing and potentially private characteristic that is unique to the requesting agent. Types of evidence have included worn insignia, secret phrases, official certificates,

identity documents, spoken passwords, and branded skin. In the digital age, experts in computer security agree upon three primary classes of unique characteristics which are admissible as evidence (Gollmann 2011, 59–62). Termed authentication *factors*, these are:

(1) *Factor 1: Something you know*—such as a password or a bank PIN number
(2) *Factor 2: Something you have*—a physical object, for instance, a smart card that provides access to your office
(3) *Factor 3: Something you are*—biometric information such as fingerprints and gait.

Computer authentication systems may request one or more of these factors from an agent, and these factors must be used in conjunction if the authentication request is to be successfully submitted. For instance, banks deploy multifactor authentication solutions in ATMs. To make a cash withdrawal, an agent must supply a bank card (something you *have*) and a PIN (something you *know*). The more factors required, the more secure the authentication process is considered to be.

The following subsections provide examples of three commonplace authentication trust systems. I explain how each technology operates as a trust system by analyzing the interplay of trust, identity, and evidence in each case.

Username and Password

Computer passwords may be likened to the basic security offered by a combination padlock on a gym locker. The padlock can only be unlocked by the person who knows the secret code. Passwords became popular in IT with the invention of computer "time-sharing systems" in the 1960s. These were computers capable of letting multiple users interact with them concurrently. While each user could access their files on the server with a *username*—a short public code by which an agent asserts their identity to a system—the system architects at MIT created the Compatible Time-Sharing System which was the first to implement a mechanized "lock" which ensured "a degree of privacy and separation between different people's work" (Smith 2002, 10). Along with their username, time-sharing system users were required to enter a "private code" or password to login. The fundamentals of this early password mechanism are as follows:

> The computer asks the person to type in a user name and password. The computer searches the system's password file for an entry matching the user name. If the password in that entry matches the password just typed, then the login succeeds. (Smith 2002, 10–11)

This basic mechanism has evolved in sophistication over time to combat the many types of attacks that are designed to steal passwords and use them to gain unauthorized access to resources. To prevent "shoulder surfing," for instance, modern computers will not display the real password being typed but instead show each character as a star ("*"), thus ensuring the password cannot be read off screen by someone peering over a person's shoulder.

Computer authentication also uses *hashing* to protect the storage of user credentials. While access to the password file was typically restricted, its contents were initially stored in plain text, making the file easily readable by any intruder who could lay hold of it. Rather than transmitting and storing passwords in plain text, computer systems nowadays use a mathematical hash function to convert the password into a long series of letters and numbers (a "digest"). Hashes act as "one way locks" because intruders cannot easily reverse their operation to retrieve the original plain text password (Gollmann 2011, 56).

As an authentication method, username and password represents a simple computerized trust system. An *identity* is claimed by the agent in asserting a username; the *evidence* to support that claim is the password. The system *trusts* the identity claim only if the password entered corresponds to the hashed password it holds on file for that user. Yet this trust relationship is easy to compromise. Passwords can be stolen if the password file is stored in plain text or if humans choose passwords which can be easily guessed. The use of mathematical encryption algorithms (such as hashing) to protect password files is now commonplace, but with enough time an attacker may still decrypt a hashed password (Grove 2000, 339).

Biometric Self-Authentication

Security experts have long lamented that a drawback of simpler authentication methods is the need for the human agent to provide evidence in the form of something they know or have. This evidence is a weak link—anybody could login "as you" if they know your password. Enter biometric authentication. On the premise that it is harder to steal or forge something *you are*, "biometrics" aims to enhance security and access control by getting a human agent to self-authenticate using a unique personal physiological or behavioral characteristic of themselves, whether face, voice, iris, or fingerprint (Wayman 2005, 1–5). To cite a stock example, San Francisco International Airport uses biometric self-authentication: hand geometry readers control employee access to secure areas. It works by having agents enroll onto the system by providing an initial sample of the required physiological characteristic. Future samples submitted to the system will be verified against the stored template for that person.

This use of body biometrics represents a relatively simple trust system. The agent's identity claim, and the corroborating evidence, is submitted

to the system as one item, namely, a sample of the requested physiological trait. The system will trust the submitted sample only if it matches the system-held template for that person. Although considered more convenient and secure than traditional authentication methods, body biometrics cannot eliminate the potential for doubt and deception: physiological information is open to forgery; personal traits such as fingerprints and voice can be copied and reproduced by attackers (Smith 2002, 195–96). Moreover, while stolen passwords can be reset, physical traits such as fingerprints, once compromised, cannot be amended or updated. To mitigate against this risk, biometrics are often used in combination with other factors of authentication.

Public Key Infrastructure

PKI is the most complex authentication trust system reviewed here. PKI is often used by IT departments in large organizations to ensure that electronic interactions—such as the sending and receiving of email—can take place securely, privately, and at scale between verified computers and users (Adams and Lloyd 2011, 195). PKI attempts to overcome the confidentiality and security loopholes inherent in simpler authentication systems by automating the verification process. It achieves this by implementing a combination of objects and relationships including "public key pairs," "digital certificates," "certificate authorities," "ciphers," and other technologies. These work together in the background, normally without any human intervention, to establish trusted identity between devices and user accounts.

Consider this example. Alice and Bob work for Corporation X and want to send each other confidential emails. PKI facilitates this by providing each of their computers with a mathematically linked "key pair"—one "public" one "private" (Adams and Lloyd 2011, 12). With this technology, Bob's computer will encrypt his email message to Alice using Alice's public key in the safe knowledge that it can only be decrypted by Alice's computer using her private key. So long as Alice's private key is not stolen, Bob's communications to her are secure.

But how can Bob be sure that Alice's public key is really Alice's, and not an imposter's? The job of digital certificates is to verify the identity of the public key holder (Adams and Lloyd 2011, 69). Each certificate specifies a public key along with the identity it is associated with. This information can be trusted assuming the certificate itself has been issued by a trusted source, a recognized certificate authority. We can trust what the certificate says about its issuer by referencing its "digital signature"—a hash that can be checked to confirm that the certificate's information has not been tampered with.

Case Study: DSA and Computer Authentication Trust Systems

Previous sections examined how computer science and theology each approach the problem of authenticating identity. Readers will hopefully have gleaned not only how authentication is a topic of importance to both disciplines, but also something of the very different assumptions, understandings, and methods each brings to the verification of identity. Despite these differences, the following discussion illustrates how theologians can use the resources of computer science to better explore and explicate the idea of divine self-authentication. Indeed, what does the divine act of self-authentication look like? What role does God give to evidence in this act? And why, despite DSA, does the threat of doubt and deception about divine identity persist? The following three subsections showcase the contribution computer science makes to our understanding of the nature, evidence, and efficacy of DSA.

Modeling the Nature of DSA with Computer Trust Systems

Theological reticence regarding the nature of DSA has its roots in the classic view, advanced by Calvin and Barth among others, that although an anchor of the Christian life, the redemptive work of the Holy Spirit is secret and incomprehensible; it is a miracle and mystery that defies human attempts at explication (Barth 1956, 648–49; Calvin 1960, 462). Yet one problem with this classic standpoint is its distinctly uneven approach to setting the limits of legitimate theological description. Within the Reformed tradition, lengthy volumes are dedicated to exploring the inner life of the Trinity, so it is curious that the human-facing epistemological work of the Holy Spirit is ruled off-limits as something about which comparatively little can be said. Challenging that reticence, this section considers the novel contribution computer science makes to our understanding of the multiform nature of God's act of self-authentication.

We begin by noting that while existing studies of DSA have increased contemporary theological interest in DSA, none of them attempts to describe what is happening *operationally* on the divine-side when God executes this act. So how might theologians best represent and account for the multitude of ways and forms by which God is said to verify his identity to humans? The proposal here is that computer-based trust systems offer a high-level schematic for elucidating the complex, rational, and multiform nature of DSA. This is to suggest that trust systems function as a "disclosure model" for DSA (Kallenberg 2015). Such models are valuable because they allow researchers to analogically represent or make intelligible something which would otherwise lie beyond description and imagination, in this case, the variegated structural patterns of DSA.

We might unfold this point by noting that in our earlier study of computer authentication systems, we saw that while a user may subjectively experience authentication as a single act of logging on to a computer using a username and password, the reality behind the scenes is much more complex. The target system will attempt to verify an agent's identity using an underlying technical infrastructure that is responsible for processing authentication requests. These infrastructures are systems which check evidence to see if it corroborates the identity declared by the username. Such trust systems are capable of incredible complexity. Consider again PKI: an *identity* is claimed via the public key, which is associated with a user account or a machine; the *evidence* is the digital certificate, which if intact verifies the identity of the public key owner; and *trust* is established by way of cross-validation checks between keys, devices, certificates, and the certificate authority. There are clearly several interrelating and interacting objects and relationships which must all work dynamically together to judge an authentication request when it is received.

In epistemological readings of the Bible, by comparison, acts of DSA are presented as events which take many different forms. However, we might say that underlying these events is a "trust system" of sorts, too—an expansive ontological infrastructure consisting of a selected set of dynamically interacting spiritual and creaturely objects which cooperate upon divine command to authenticate God's identity in a chosen way to a target audience. If epistemological readings of the Bible are accurate, a single instance of DSA seemingly requires for its execution clusters of objects, which are formed into human-perceptible events such as miracles. The objects used in DSA vary, and have included human cognition; a particular space-time setting; animals and elements of the natural world; church teaching and practice; prophetic and apostolic witness; conscience; the testimony and insight of family, friends, enemies, and strangers; dreams and imagination; personal suffering or success—and a whole host of other environmental, personal, and spiritual variables. What happens in DSA is that God harnesses objects from various ontological domains, singularly or in combination, to accomplish the goal of establishing human assurance about his identity and intentions.

God's use of varying combinations of objects means that the act of divine self-authentication does not have a singular pattern of execution. If Biblical accounts of DSA are an accurate guide, then God authenticates himself in different ways to different people at different times. Thus, there are myriad authentication patterns the act could potentially implement, each with a bespoke arrangement of objects and a unique divine identifier.

An arising question is what determines God's choice of one structural pattern over another? To answer that, we might note that variegated structural patterns in computer trust systems are not random but preplanned choices. They allow the authentication workflow to be flexibly altered

depending on *who* is being authenticated, *where* authentication is taking place, and for what *purpose*. Consider how the workflow changes when setting up a payment in your banking app: there is one authentication step if the payee is known, two if they are not, and three if the setup is being done on a public computer. The suggestion here is that variegations in the structural patterns of DSA are similarly deliberate rather than capricious or random: God modifies the authentication workflow depending on the context and purpose of his act of self-authentication. In other words, God's object selection logic takes into account target-side factors. The act of DSA—including its message and mode of delivery—is deliberately tailored to fit the recipient's life situation and epistemic needs.

While further work is needed to understand the possible and legitimate extent of the trust system model's applicability to this aspect of divine action, an important qualification ought to be made now. While computer trust systems are often automated, programmed, and impersonal, DSA is a free act of God which is both personal and transformative. The Biblical witness suggests that the act in which God confirms himself to believers is not automatically triggered or executed, nor the outworking of an impersonal system process. It is an act in which God the Holy Spirit is said to be fully and personally present to the recipient in and through the dynamic constellation of cross-domain objects God has chosen to bear witness to himself. It is a personal act of communication. We might therefore say that DSA is *like* a computer authentication trust system in as much as both are purposive, coordinated, multiobject and multiform acts.

Forms and Functions of Evidence in DSA

If accepted as valid, the trust system model is capable of analogically representing key aspects of the nature of DSA, such as its variegated structural patterns. But can this model be extended to account for the *evidence* God supplies to humans in acts of DSA? Do computer authentication trust systems, in which evidence has a distinct range of types and roles, shed any light on the forms and functions of evidence in DSA? Or are their accounts of evidence so dissimilar that here, at this point, we are forced to concede that the analogy between them breaks down?

In our earlier analysis of computer trust systems, we saw that evidence is always required to verify an identity claim, and that such evidence is broadly defined as a distinguishing and potentially private characteristic that is unique to the requesting agent. Such evidence functions as a unique identifier or "truth indicator," signaling to the computer system whether the submitted identity claim should be regarded as valid and correct. The types and quantity of such evidence varies depending on multiple criteria such as the importance assigned to the target system it guards access to. In addition, we noted that there are three classes of evidence a system may

request: something you *know* (a password or PIN), *have* (an entry card or bank card), or *are* (a physical or behavioural characteristic). The sorts of evidence requested by a computer system is thus finite and well-understood. Indeed, the list of valid and acceptable evidence types is planned and preprogrammed by system architects and software developers, who will also implement standards and protocols to ensure that evidence is requested, collected, processed, and stored in an appropriate manner.

There also appears to be a well-defined, if contested, range of evidence types which support the religious belief that God is who says he is: "arguments," "religious experience" of assurance, "testimony," and "personal transformation" are variously cited by believers as evidence that entitles their belief that God is known and can be trusted (Smith 2014). Regardless of the evidentialist critique that arguments and testimony are inherently weak types of epistemic justification, a problem with these standard evidence types is that they are manufactured by humans externally to the act of DSA. Given that DSA has been described throughout this study as an act *within which* God deploys evidence to confirm his identity, it is suggested that the truth indicator must somehow be intrinsic to the Holy Spirit's work of self-witness. But which specific aspect of that work authenticates the truth of divine identity to humans?

Here several possibilities emerge. One, which we shall discuss in the next section, is that God's identity is such that it always and irresistibly authenticates all divine action as being from God. In that rendering, the truth indicator is God's being *in se* and *pro nobis*. A second and related contention is suggested by PKI: just as authentication occurs when linked key pairs are used to send/encrypt and receive/decrypt messages, so the authentication of God's identity occurs in the "match" or "proper fit" that the Holy Spirit effects between divine speaking and human hearing, between God's message of grace and the recipient's awareness of their need for grace.

Another place to look for a truth indicator of divine identity is in the creaturely evidence God himself marshals in support of his own identity claims. As we have seen, specific acts of DSA are divinely initiated events consisting of unique clusters of objects which are so arranged by the Holy Spirit to display and confirm the truth of some aspect of God's identity and character to the human knower. Questions native to this second line of enquiry include: is there a typical range of objects God uses to display and confirm his identity? And are there any discernible patterns to evidence formation that might allow researchers to better discern, understand, and potentially even predict acts of DSA?

In telling of God's acts, the Bible appears to offer a promising starting point for that analysis. Yet the Bible itself also cautions that there are insurmountable barriers to producing a complete catalog of which objects count as evidence. The Psalmist's proclamation that "the firmament

proclaims [God's] handiwork" (Psalm 19:1 NRSV) lends credence to the idea that any or all creaturely objects may in fact be utilized by God to communicate and confirm his identity. This brings an almost infinite range of objects into play, with no evident limit set on viability, and nor then on the patterns of evidence-cluster formation at God's disposal. This leaves researchers with no accurate baseline from which to benchmark which object-clusters are used in which authentication scenarios.

A second barrier to finalizing what counts as evidence of divine identity relates to the idea discussed in the previous section that God intentionally varies the selection of objects according to (1) the specific message of assurance to be conveyed and (2) the recipient's life situation and epistemic needs. If the evidence deployed in each act of DSA is so personalized as to neatly fit its target, then common agreement about what counts as evidence of divine assurance in any given case may not be possible. The target may cite evidence to justify their belief, but the bespoke nature of that evidence (and of its mode of delivery) may make it unverifiable or unacceptable to independent onlookers.

The ambiguity surrounding the range and admissibility of evidence types in DSA stands in clear contrast to the strict and well-defined approach to evidence within computer authentication systems. But far from only serving up points of dissimilarity, however, computer science also casts fresh light upon a similarity in the evidence used in both DSA and computer authentication, namely, the importance of its temporary and single-use character.

To offset human weakness, authentication evidence has become increasingly time limited and single use. Login passwords and the digital certificates used in PKI may have an expiry date after which a new one must be created. An online banking pass code only works if used within a short timeframe and cannot be reused in subsequent authentication requests. Similarly, some of the evidence God deploys in acts of DSA may also be temporary and/or single use. The Bible is replete with examples of temporary evidence: the burning bush does not burn away endlessly; Jesus' storm-calming does not permanently alter the weather above lake Galilee. Moreover, these and other miracles through which God confirms himself to the Israelites are also single use in as much as their structural pattern, that is, the arrangement of creaturely objects through which God miraculously self-manifests, is often never repeated.

From the standpoint of Reformed doctrine, the idea that God uses creaturely objects in a singular and temporary fashion to bear evidential witness to himself is not entirely new. Indeed, in his theological epistemology of the *Church Dogmatics*, Barth acknowledges these properties of divine action and sheds valuable light on their intended purpose. He advances the concept of a "dialectic of veiling and unveiling" according to which God is able to "commandeer" creaturely objects to reveal himself

in such a way that does not annul his hiddenness (Barth 1957, 199). In Barth's view, creaturely objects do indeed bear witness to God, but the manner of their commandeering is temporary and singular. Their witnessing role is temporary in as much as it is only activated and deactivated upon divine command, and may also be singular if deemed nonrepeatable and nonreplicable—a status Barth uniquely assigns to the singularity of Christ's incarnation, life, death, and resurrection.

Yet Barth does not pitch his affirmation of the temporary and single use character of witnessing objects as a human theory about divine action. He regards them as features intrinsic to God's self-revelation toward humans. These two properties testify to God's absolute freedom in relation to the human knower. They render divine action a finite, bounded *event* in human space and time—one with a trigger, form, and duration solely controlled by God. The object clusters used by God in events of DSA thus never become fixed data points under human control but are always provisioned and withdrawn from service by God's own command.

It is worth pointing out that theological systems which do not operate with an event-based conception of divine self-revelation may allow for other DSA evidence types that Barth would likely reject, such as those offered by "natural theology"—an approach to theology which advocates that embedded within creation are fixed touchpoints for divine revelation that are open to discovery and analysis by human cognition. The list of potential touchpoints varies across and within Christian traditions but typically includes the natural world, aspects of human reason and experience, and even the life of the saints (Harrison 2017). For Barth, however, the idea that genuine knowledge of God can be readily accessed and authenticated by humans independently of God's own act of self-revelation is a nonstarter. His counterproposal is that the only "point of contact" between God and humanity by which genuine knowledge of God is produced and posited is the divinely instigated "analogy of faith"—an event in which the Holy Spirit, working in tandem with the Bible, miraculously bridges human hearing and divine speaking such that despite their dissimilarity humans become able to hear God's Word of grace to them (Barth 1936, 236).

DSA and the Continuing Problem of Deception

Far from resulting in human trust and confidence in God, epistemological readings of the Bible indicate that acts of DSA are often prone to failure: people are not in every case convinced by God's work of self-authentication; DSA has not been experienced by all Christians; and moreover, the Bible points to the existence of a continued threat to human assurance about God's identity in the form of malevolent agents. While the ongoing threat of deception about God's identity may never be fully

eliminated, is there anything to be learned from computer authentication systems about how to better manage this risk?

Computer science takes a pincer approach to the threat of doubt and deception: it (1) establishes ways of *officially certifying* trusted sources and (2) implements *practical measures* to prevent imposters from successfully authenticating. As regards (1), we saw how PKI establishes trusted source using a combination of digital certificates and key pairs. The certificate can be trusted if its hashed digital signature has not been tampered with. Regarding (2), measures are implemented to detect and patch the technical vulnerabilities an attacker could exploit to gain unauthorized access to a system. As we saw, examples of attack vectors are holding a password file in plain text or issuing only a single mathematical key for encrypting and decrypting emails.

Could theology adopt a similar pincer-style approach to the problem of doubt and deception? The following two subsections offer a reflection on that possibility.

Certifying Trusted Divine Source. The problem of trusted source is ever-present in the human domain: computer-based authentication will be successful if the evidence supports the identity claim, but such systems cannot judge whether the *source* of the claim is in fact genuine. Indeed, the person or device asserting an identity is not necessarily who they claim to be—it is possible for an imposter to authenticate if they have what the system is looking for. With regards to divine identity, the main Church traditions have long certified the Bible as a trusted primary source of the knowledge of God. Yet here emerges the same problem that blights human authentication: on what grounds can and should a believer trust that the divine claims revealed in Scripture are made by the God of Abraham, Isaac, and Jacob, and not by a *daemon*?[2] And by extension, what guarantee is there that acts of DSA have not been intercepted and tampered with by malevolent spiritual forces?

The Reformed tradition proposes a doctrinal answer to the question of trusted divine source—one that is located deep within actualistic accounts of divine identity. A contention of Barth's is that Christians can trust that God is who he reveals himself to be in the Bible because divine revelation is *self-certifying*, since according to the Bible God is "not another than He is in His works" (Barth 1957, 260). Divine revelation produces true and trustworthy knowledge for humans precisely because it is God's "*self*-revelation" (van der Kooi 2005, 438). By this statement, Barth means that God's revelation of himself is genuine on its own because of the unique shape of God's identity: unlike human identity, divine identity has a form that is intrinsically self-authenticating.

To elaborate, human identity comprises three distinct elements which are all capable of being detached from each other: "person," "action," and

"speech" (Torrance 1971, 141). It is the divided or *modular* nature of human identity, Torrance asserts, that prevents human acts and speech from being truly self-authenticating, primarily because it entails that they are not always and indubitably related to the person who performed and uttered them—even a person's physical presence to another is not enough to truly guarantee they are who they say they are. To be sure, one person can impersonate another; the acts and speech of one person can be transposed or attributed to another; and unique identifying traits of a person can be stolen, reproduced, and fraudulently used by another.[3] Thus pictured by Torrance, human identity possesses an in-built security vulnerability that begets the need for systems of authentication: unable to ontologically certify the truth of their identity, humans are left to find means of judging how and whether to trust each other's identity claims.

In sharp contrast, divine acts are inherently self-authenticating because God's identity is undivided: there is no cleft between God's person, speech, and acts. Indeed, God's acts and speech always "coincide in the unity and power of his person" (Torrance 1971, 141). For Torrance as for Barth, this unity of identity is predicated on the idea that God is a *being-in-act*, which is to say that God's being and act are identical, existing in inseparable ontological and epistemological integration. As there is no possibility of incongruence, division, or distance between God's being and God's act, believers can trust that God really is the person the Bible pictures him to be, namely, "the God who loves in freedom" (Nimmo 2007, 7).

An upshot of the preceding analysis is that, unlike human authentication which involves judging an identity claim for its validity, DSA results in true assurance about divine identity because in divine action the recipient is never presented with a mere verbal or written claim but is always and indubitably confronted with the person *behind* the claim, namely, God himself as revealed in Jesus Christ. DSA thus generates human assurance about God because it is a class of divine acts in which God the Holy Spirit witnesses to the person and work of God the Son and speaks this self-witness to the human recipient person-to-person, as it were, in the undivided unity of God's being-in-act.[4]

Some Practical Measures. As just described, it is the undivided nature of God's identity which conditions the possibility that divine action (including specific acts of DSA through the Holy Spirit) is self-certifying, i.e., authenticates itself as coming from a trustworthy divine source. Yet this claim appears to suffer serious challenge when tested for *ecological validity*, that is, when tested for its validity and applicability in real-world settings. How valid is the doctrinal contention that specific divine acts (Type 1 DSA) or divine action more generally (Type 2 DSA) are always and

everywhere self-authenticating when evaluated in the real-world contexts in which God puts it to work?

When so tested, the prognosis for DSA is not unassailably positive. For as we saw in an earlier section, acts of DSA are not in fact always and everywhere convincing. Acts of divine self-authentication are often seen to fail, are not experienced by all believers, and despite them the risk of doubt and deception about God's identity continues to persist among God's people. It is quite clear that to establish trusted divine source, identity certification initiatives at doctrinal level—such as that described in the previous section—need paired with practical measures that will somehow support humans in the real-world challenge of perceiving and recognizing genuine divine activity.

One such practical measure is illuminated with reference to a recent advance in biometric authentication technologies. There is a growing trend toward building *wise* biometric systems. Such systems train themselves to recognize genuine user access requests. So-called "continuous authentication" systems use artificial intelligence to monitor and learn about a user's activity. They attempt to develop a more holistic and continuous view of user behavior on which to make more reliable authentication decisions (Dasgupta et al. 2017, ch.5). Consider a purchase made abroad with the banking app on your phone. Alongside evaluating the veracity of the physiological trait used to log into the app, the bank's authentication system will factor in behavioral characteristics to reduce the risk of fraud. These might include a user's location, the time of purchase, credit card usage patterns, and even pin and password typing style. Self-training authentication systems like these constitute complex trust systems that aggregate multiform evidence, gathered across an ever-broadening time slice, into optimized authentication judgments.

In a similar vein, albeit in the realm of analytic theology, it has been argued that continuous training or learning about God may likewise improve a religious knower's capacity to detect and differentiate genuine divine activity from the activity of imposters. Referencing Coakley's work on the "spiritual senses" tradition, a recent study by McGuigan and Kallenberg makes the point that habituated bodily practices such as meditation and contemplation may train, and thereby optimize, the perception of a religious knower to "better" (i.e., more accurately or "truthfully") perceive God's presence and activity (Kallenberg and McGuigan 2017). It is reasonable to infer that this training could in their view, under the right conditions, also result in wiser authentication judgments. If, as they suggest, perceptual optimization does increase through habituated mystical practices, then one would expect to see a corresponding rise in detection rates for nongenuine and genuine divine activity alike.

If training of this sort is the first practical measure a religious knower might take to support their perception of genuine divine activity, a second

relates to the choice of context in which they come to make authentication judgments, i.e. decide whether perceived divine activity is genuine or not. In contrast to the individualism that often marks accounts of religious knowing, Coakley draws attention to the valuable role "religious communities" play in nurturing the practice of perceiving God (Coakley 2009). Apart from the medieval spiritual sense communities Coakley has in mind, we may observe that churches down through the ages have provided a space within which collaborative learning about God takes place at depth and scale, and in which a variety of practices and forms of knowledge—beyond the mystical and noncognitive—are warranted and welcomed for use in the knowing of God. Churches of all traditions offer a broad range of established "ecclesial practices" that can be harnessed singly or in combination by community members to better judge the presence of genuine divine activity. Practices include the public reading of Scripture, prayer, Eucharist, homilies, pastoral care, outreach, and acts of service and mercy.

In Coakley's view, however, ecclesial practices have a critical role to play in the authentication of divine identity beyond the mere training of a religious knower's perception. Ecclesial practices provide a valuable communal means of adjusting for, and safeguarding against, errors in the practice of perceiving God. They offer a "vital bulwark against error" (Coakley 2009, 305). A network of trusted people and practices has the potential to facilitate rigorous epistemic testing of a person's authentication judgments about divine identity.

Conclusion

The foregoing analysis illustrates how the contributions of computer science on authentication can deepen theological reflection upon the nature, evidence, and efficacy of DSA. Computer authentication trust systems offer a means of analogically representing and accounting for the variegated structural patterns of this highly dynamic divine act. Computer science also provides a useful foil for theological reflection upon what counts as evidence of divine identity and draws attention to the importance of its temporary and single-use character. The acknowledgment that acts of DSA are, by divine design, not wholly efficacious also led us to review how the continuing risk of deception about God's identity might be offset using strategies and practical measures informed by computer science.

Dialogue between theology and computer science is at a very early stage, and so it is hoped that these findings will inspire further collaboration. There are several ways in which the current study of authentication could be jointly extended.

One arising question is whether there is a computer authentication trust system which more accurately models DSA activity. The three trust systems examined here were chosen because they are commonplace and

comprehensible to the nonspecialist reader, but other more technically complex options do exist. For instance, it may be instructive to review Security Assertion Markup Language (SAML) which is a standard governing the secure exchange of authentication data between web-based applications.

Another future line of research might examine whether the trust system model could be extended to account for how God ensures messages of confirmation are received by the target audience without interception and interference by malevolent spiritual or human agents. The issue of how divine communications are secured and made secret could be profitably explored with the support of *cryptography*—the science of "making information unreadable by unauthorized persons" (Grove 2000, 339).

A third line of enquiry could develop the "human-side" analysis of DSA, a topic which fell outside the scope of this article. A strand of that work would connect analysis of the evidence types used by God in DSA to the ongoing debate within the epistemology of theology about the justificatory role of evidence. What impact does the temporary and single-use character of DSA evidence have on the subordinate role Reformed theologians traditionally assign to evidence vis-à-vis faith as that which warrants a believer's trust in God? Do these two features lend support to a moderate evidentialist account of religious belief such as that outlined by Martin Smith (Smith 2014)?

In finishing, there are several noteworthy challenges inherent in the use of computer system analogies to represent divine action. The first of these was mentioned earlier and concerns how to let such analogies illuminate a dimension of divine action without raising the twin specter of *impersonalism* and *involuntarism*. For if applied too rigidly and extensively, the systems motif will invariably eclipse the personal, dynamic, free, and loving nature of God's action toward humans.

A second challenge in presenting a schema to account for some aspect of divine action is that it draws attention to *how* God communicates at the expense of *what* he communcates—a move that is sure to ignite old epistemological anxieties within Reformed theology. Although a premise of this article is that the how of the Holy Spirit's work of assurance can be fruitfully elucidated using modern conceptualities, the very legality of such an approach is open to dispute, especially if the limits of theological description are set such that the Spirit's work is deemed an indescribable, inexplicable mystery of grace.

A final, if more general, anxiety centers upon how to test human images of divine action—including the one presented here—for their validity. Proponents of a critically realistic theological epistemology, such as Barth and Torrance, would contend that human images of the *how* are invalid when used as the primary entry point into an analysis of the nature of divine action. To be valid, human images must be shown to have received

their foundation and form from within the concrete message (the *what*) of God's self-communication. The truth and accuracy of human images is therefore judged by whether—as limited human attempts to conceptualize the divine—they arise as responses which obediently "think after" [*nachdenken*] God's self-revelation in Jesus Christ as perceived by the human knower through the interplay of Spirit and Word (Barth 1936, 25).

Notes

1. For instance, in modern Catholic theology, von Balthasar proposes that the trustworthiness of divine revelation is rooted in the self-authenticating "glory" of God. Revelation manifests the "glorious majesty" of divine love, which when experienced "leaves one no choice but to respond in the mode of pure, blind obedience." von Balthasar (2004). *Love Alone Is Credible*. San Francisco, CA, Ignatius Press.
2. For a philosophical take on why it might be impossible to authenticate divine revelation, see "Authenticity of Divine Revelation," at https://rationalwiki.org/wiki/Authenticity_of_divine_revelation.
3. It is precisely in view of this very security vulnerability that well-implemented computer authentication systems do not simply accept a stand-alone identity claim but will mandate the submission of corroborating evidence.
4. A consequent point of contrast is the differing strength given to "personal communication" in divine and human authentication strategies. DSA is a personal (and "person-to-person") communication that is, if Torrance and Barth are correct, fully self-authenticating. By contrast, physical person-to-person interactions between humans are not by themselves self-authenticating, with security experts considering them a weaker and more precarious form of claims-based authentication than the methods offered by computer authentication systems.

References

Adams, Carlisle, and Steve Lloyd. 2011. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. London: Addison-Wesley.

Barth, Karl. 1936. *Church Dogmatics*, Vol I/1. London: T & T Clark.

———. 1956. *Church Dogmatics*, Vol IV/1. London: T & T Clark.

———. 1957. *Church Dogmatics*, Vol II/1. London: T & T Clark.

Bishop, Matt. 2003a. *Computer Security: Art and Science*. Boston: Addison-Wesley.

———. 2003b. "What is Computer Security?" *IEEE Security & Privacy* 1 (1): 67–69.

Calvin, John. 1960. *Institutes of the Christian Religion*. Louisville, KY: Westminster John Knox Press.

Coakley, Sarah. 2009. "Dark Contemplation and Epistemic Transformation." In *Analytic Theology: New Essays in the Philosophy of Theology*, edited by Oliver D. Crisp and Michael C. Rea, 280–312. Oxford: Oxford University Press.

Dasgupta, Dipankar, Arunava Roy, and Abhijit Nag. 2017. *Advances in User Authentication*. Cham: Cham, Switzerland: Springer International Publishing.

Diller, Kevin. 2014. *Theology's Epistemological Dilemma: How Karl Barth and Alvin Plantinga Provide a Unified Response*. Downers Grove, IL: IVP Academic.

Gollmann, Dieter. 2011. *Computer Security*. Chichester, UK: Wiley.

Grove, Ronald. 2000. "Fundamentals of Cryptography and Encryption." In *Information and Security Management Handbook*, edited by H. Tipton and K. M. London. Boca Raton: Boca Raton, FL: Auerbach.

Harrison, Victoria S. 2017. "Hans Urs von Balthasar". In *The Oxford Handbook of the Epistemology of Theology*, edited by W. J. Abraham and F. D. Aquino. 535–47. Oxford: Oxford University Press.

Healy, Mary and Robin Parry, eds. 2007. *The Bible and Epistemology: Biblical Soundings on the Knowledge of God*. Milton Keynes, UK: Paternoster.

Kallenberg, Brad. 2015. "Some Practices of Theological Reasoning, or, How to Work Well with Words." In *The Routledge Companion to the Practice of Christian Theology*, edited by M. Higton and J. Fodor, 35–54. London: Routledge.

———, and Colin M. McGuigan. 2017. "Ecclesial Practices". In *The Oxford Handbook of the Epistemology of Theology*, edited by W. J. Abraham and F. D. Aquino, 141–56. Oxford: Oxford University Press.

Moser, Paul. 2017. "The Inner Witness of the Spirit". In *The Oxford Handbook of the Epistemology of Theology*, edited by W. J. Abraham and F. D. Aquino, 111–24. Oxford: Oxford University Press.

Nimmo, Paul T. 2007. *Being in Action: The Theological Shape of Barth's Ethical Vision*. London: T & T Clark.

Pelikan, Jaroslav. 1989. *The Christian Tradition: A History of the Development of Doctrine*, Volume 5. Chicago: University of Chicago Press.

Plantinga, Alvin. 2000. *Warranted Christian Belief*. Oxford: Oxford University Press.

Rae, Murray. 2007. "Incline Your Ear So That You May Live: Principles of Biblical Epistemology." In *The Bible and Epistemology: Biblical Soundings on the Knowledge of God*, edited by M. Healy and R. A. Parry. Milton Keynes: Paternoster.

Smith Martin. 2014. "The Epistemology of Religion." *Analysis* 74 (1): 135–47.

Smith, Richard. 2002. *Authentication: From Passwords to Public Keys*. London: Addison-Wesley.

Torrance, Thomas F. 1971. *God and Rationality*. Oxford: Oxford University Press.

———. 2000. "The Distinctive Character of the Reformed Tradition." *Reformed Review* 54: 5–16.

van den Belt, Henk. 2008. *The Authority of Scripture in Reformed Theology: Truth and Trust*. Leiden: Brill.

———. 2011. "Scripture as the Voice of God: The Continuing Importance of Autopistia." *International Journal of Systematic Theology* 13 (4): 434–47.

van der Kooi, Cornelis. 2005. *As in a Mirror: John Calvin and Karl Barth on Knowing God*. Leiden: Brill.

von Balthasar, Hans U. 2004. *Love Alone is Credible*. San Francisco: Ignatius Press.

Wahlberg, Mats. 2020. *Divine Revelation*. The Stanford Encyclopedia of Philosophy.

Wayman, James. 2005. *Biometric Systems: Technology, Design, and Performance Evaluation*. London: Springer.