

Comparison of Expert Declarations

Examples of Additional Similarities Not Captured by Automated Comparison Tool

Reddy Declaration ¶ ¶ 56-57

configuration.”); Cromer at 2:8-11 (“Trusted Computing Platform Alliance (TCPA)” is now “currently referred to as the Trusted Computing Group (TCG)”).; Yan at [0003]-[0004] (same). In this way, a device’s posture credentials would be formatted at the device consistently and contain substantially the same information, regardless of the device manufacturer or components operating on the device. It would also allow Gleichauf’s policy server to process posture credentials that were received, in a trusted manner from a device, more efficiently and in substantially the same way, again regardless of the device returning the credentials.

57. A POSITA would have appreciated the value of following an industry specification. It would promote interoperability among devices from different device manufacturers, so long as the devices are all specification compliant. Indeed, device interoperability is a common and important goal in computer networking.

Shields Declaration ¶ 63

2:8-11 (TCPA is the former name of TCG); EX1019, ¶¶3-4. Put differently, following the industry standard, as described in Ovadia, would benefit Gleichauf’s system by formatting a device’s posture credentials consistently and with substantially the same information, regardless of the device’s manufacturer or components. This would also allow Gleichauf’s policy server to process posture credentials that were received, in a trusted manner, more efficiently and in substantially the same way regardless of the device providing the credentials. Following the industry standard would also promote the interoperability of devices from diverse manufacturers. Ensuring the interoperability of devices is a common and important goal in the computer networking arts.

Reddy Declaration ¶ 59

59. The combination also would have been obvious because it is merely the application of a known technique (digitally signing an attestation about the state of a device to make its authentication more secure, per Ovadia) to a known method (network authorization process that analyzes a device's posture credentials that contain critical security information about the device, including its authentication, per Gleichauf) ready for improvement to yield predictable results. Here, the improvement provided to Gleichauf's process by Ovadia's digital signature technique is resistance to forged or tampered-with posture credentials. A POSITA would have been familiar with the use of digital signatures to prove the integrity and authenticity of messages or other information communicated over a network. *See, e.g.,* U.S. Patent Pub. No. 2006/0005009 at [0033] (“**To ensure that the quoted value is not corrupted during communication,** TPM 50 also can generate an attestation identity key (AIK) that is used to encrypt some or all of the quoted value. Attribute system 40 can communicate the encrypted quoted value and AIK to assurance system 42.”). Gleichauf's process is also improved because the use of a digital signature allows the policy server to authenticate that the provided posture credentials originated with the device attempting to gain access to the network. *See* Ovadia at 16:30-32 (“AS

Shields Declaration ¶ 65

65. In my opinion, the combination also would have been obvious because it applies the known technique of digitally signing an attestation about the state of a device to make its authentication more secure (as in Ovadia) with the known network authorization process of analyzing a device's security posture credentials, including its authentication (as in Gleichauf) to yield predictable results. In my opinion, a POSITA would have been familiar with the use of digital signatures to prove the integrity and authenticity of network communications and would have recognized that Ovadia's digital signature technique would improve Gleichauf's process by increasing resistance to forged or tampered-with posture credentials. EX1008, ¶33. In my opinion, a POSITA also would have recognized that use of a digital signature would improve Gleichauf's process by enabling the policy server to confirm that the posture credentials originated with the device attempting to access the network.

Reddy Declaration ¶ 68

68. The combination also would have been obvious because it is merely the application of a known technique (serving a web page with information and remediation instructions to a quarantined device, per Lewis) to a known method (providing a notification message identifying the reasons for denying a device access to the network, per Gleichauf and Ovadia) ready for improvement to yield predictable results. A POSITA would have known that serving a web page to a quarantined device from a quarantine server (with remediation instructions) would have the benefit of providing information to the user while at the same time preventing the device from communicating with network resources. Lewis at 10:61-66, 13:63-14:1. Serving a quarantine web page, per Lewis, would also be advantageous to sending a notification message, per Gleichauf or Ovadia. The redirection to Lewis's quarantine server is triggered by the user opening a browser and attempting to access network resources. See Lewis at 10:63-66 ("When client 202 is in quarantine and a user opens a web browser on client 202, QS 201 provides a web page to inform the user that the client 202 is in quarantine and corrective action must be taken."). Redirecting the device to a quarantine server and then serving a web page from the quarantine server

Shields Declaration ¶ 71

71. In my opinion, the combination would also have been obvious because it is merely the application of Lewis's known technique of serving a webpage to a quarantined device with information and remediation instructions to Gleichauf's and Ovadia's known methods of providing a notification message identifying reasons for quarantine, yielding predictable results. In my opinion, a POSITA would have known that serving a webpage with remediation instructions to a quarantined device from a quarantine server would beneficially provide information to the user while simultaneously preventing the device from accessing protected network resources. EX1006, 10:61-66, 13:63-14:1. Lewis's quarantine webpage would also be advantageous to Gleichauf's or Ovadia's notification message. Gleichauf discloses notifications in the form of "extensible messaging format, such as a Type-Length-Value (TLV) or an extensible markup language (XML) format" which "are well-defined, application independent form for representing information or data." EX1004, 20:56-60. In comparison, Lewis's webpage served by the quarantine server is displayed in the browser that a user already has opened. Therefore, modifying the XML/TVL notification approach in Gleichauf to Lewis's webpage based notifications would advantageously avoid

Reddy Declaration ¶ 69

69. Serving a web page from a quarantine server would also give the user of the quarantined device the added option to elect to proceed with the recommended remediation or terminate the connection attempt. A user attempting to access the network from a fixed location, such as an office, may have the time necessary to proceed with the remediation actions. In this instance, the web page would direct the user to a remediation server, as taught by Gleichauf, that can correct the security issue. Gleichauf at 5:4-11. On the other hand, a user that may not have the requisite time needed to remediate the security issues may elect to terminate the connection attempt. This may occur, for example, if a user is attempting to access the network from a temporary location such as an airport terminal to quickly check e-mail shortly before boarding a flight. A POSITA would have understood the benefits of giving the user a choice as to which action to take, depending on the user's own perceived need and immediacy of accessing the network.

Shields Declaration ¶ 72

72. In my opinion, serving a webpage from a quarantine server would also provide the quarantined device's user the option to proceed with the remediation or terminate the connection attempt. A user attempting to access the network from a fixed location (e.g., an office) may have time to proceed with remediation. In this instance, the webpage would direct the user to a remediation server that can resolve the security issues per Gleichauf. EX1004, 5:4-11. A user that does not have the time to remediate security issues (e.g., a user attempting access from an airport terminal) may opt to terminate the connection attempt. In my opinion, a POSITA would have understood the benefits of giving the user the option to choose their desired course of action.

Examples of Abbreviations or Slight Re-Wordings

Reddy Declaration ¶ 55

The combination would have been obvious because it represents merely the use of a known technique (Ovadia's TPM security infrastructure and digital signatures) to improve a similar method (Gleichauf's authentication and authorization of computerized devices seeking network access) in the same way.

Shields Declaration ¶ 62

The combination would have been obvious because it merely uses known techniques (e.g., Ovadia's trusted platform module security infrastructure and digital signatures) to improve a similar method (e.g., Gleichauf's authentication and authorization of devices seeking network access) in the same way.

Reddy Declaration ¶ 63

63. A POSITA would have understood that Ovadia's TPM generates and sends the integrity measurement to the authentication server because the integrity measurement is digitally signed with an Attestation Integrity Key (AIK) and "AIKs are only permitted to sign data generated by a TPM." Ovadia at 14:9, 5:35-36.

Shields Declaration ¶ 67

A POSITA would have understood that Ovadia's trusted platform module generates and sends the integrity measurement because the integrity measurements are digitally signed with an Attestation Integrity Key (AIK) and "AIKs are only permitted to sign data generated by a TPM." EX1005, 14:9, 5:35-36.

Reddy Declaration ¶ 58

A POSITA would thus have understood that the trusted computing and authentication technologies described in Ovadia are not limited to the IEEE P802.16-based networks that Ovadia describes, but instead are generally applicable to networks—like that in Gleichauf—that require authentication and authorization for access.

Shields Declaration ¶ 64

A POSITA would thus have understood that the trusted computing and authentication technologies described in Ovadia are not limited to the wireless networks Ovadia describes but instead are generally applicable to networks—like Gleichauf's—that condition network access on authentication and authorization of client devices.

Reddy Declaration ¶ 68

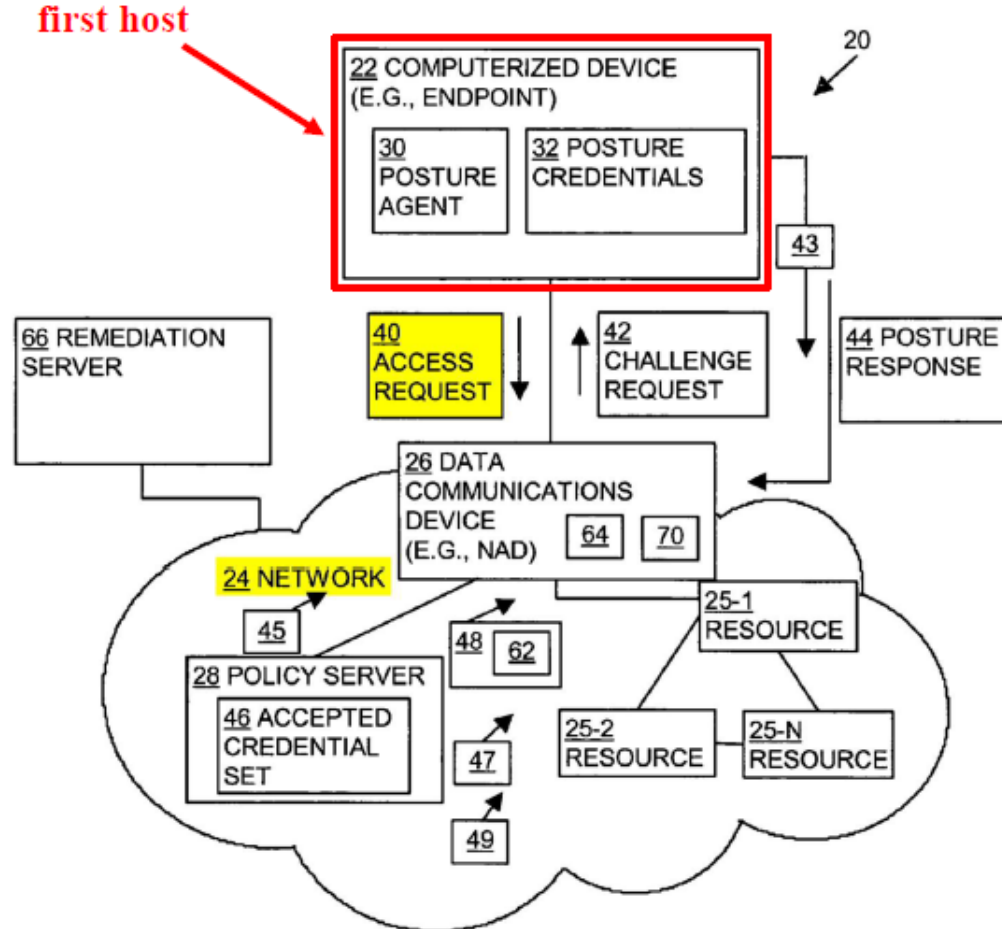
A POSITA would have known that serving a web page to a quarantined device from a quarantine server (with remediation instructions) would have the benefit of providing information to the user while at the same time preventing the device from communicating with network resources. Lewis at 10:61-66, 13:63-14:1.

Shields Declaration ¶ 71

In my opinion, a POSITA would have known that serving a webpage with remediation instructions to a quarantined device from a quarantine server would beneficially provide information to the user while simultaneously preventing the device from accessing protected network resources. EX1006, 10:61-66, 13:63-14:1.

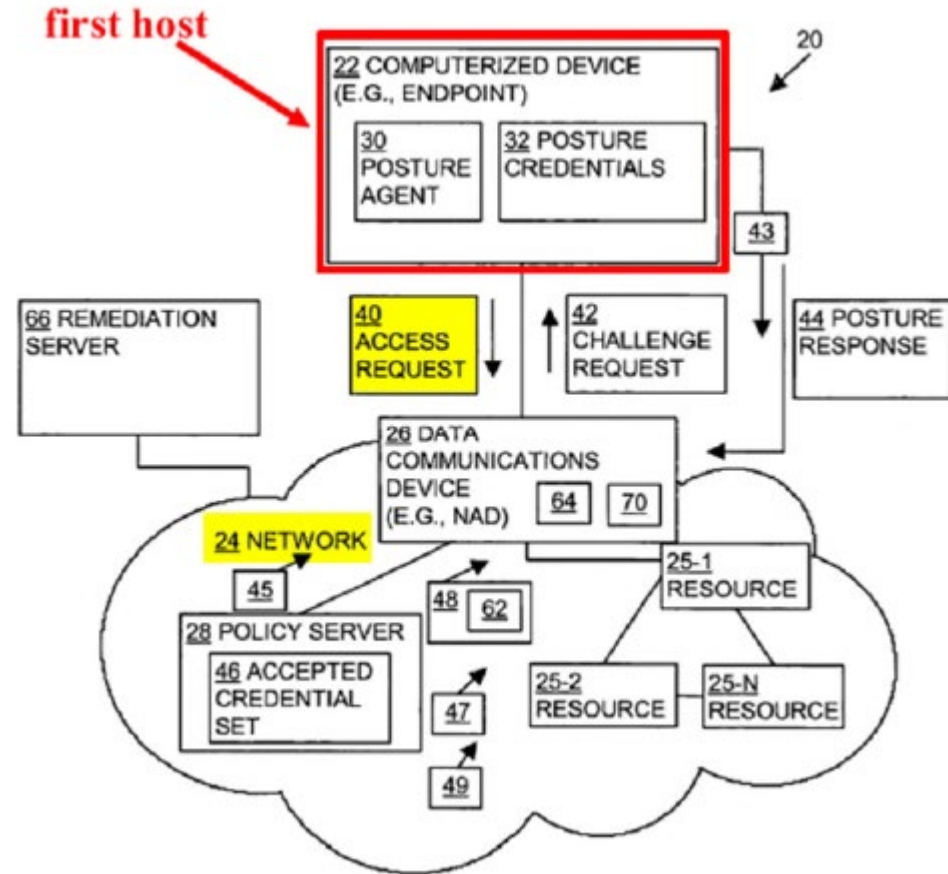
Examples of Identical Images with Identical Annotations

Reddy Declaration ¶ 80

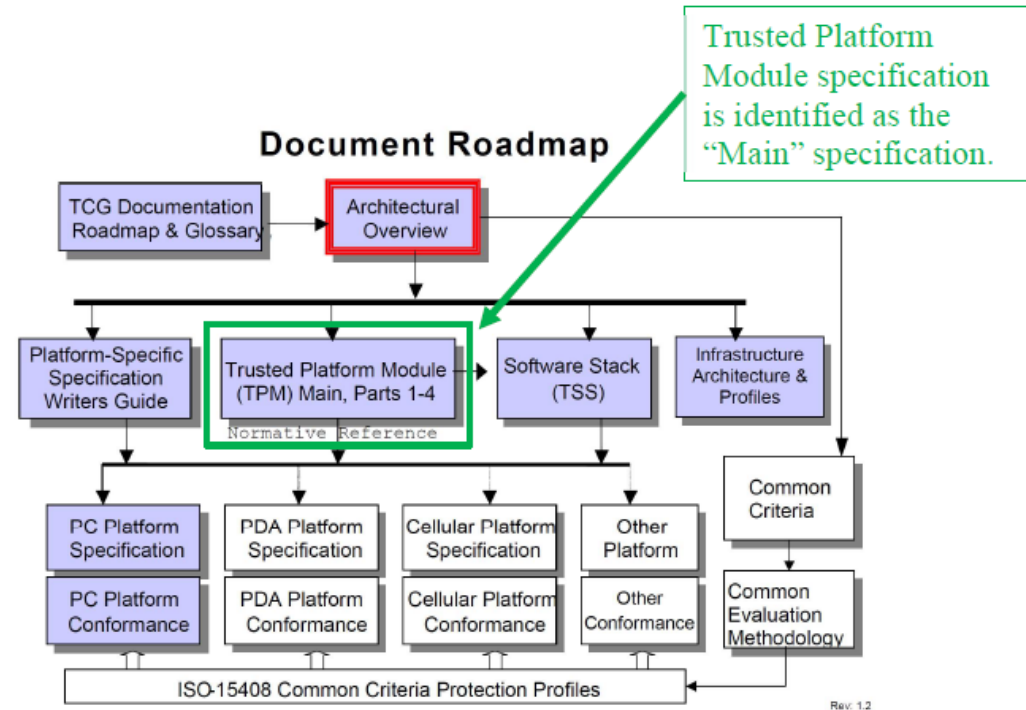


Gleiclauf at Fig. 1 (annotated).

Shields Declaration ¶ 79

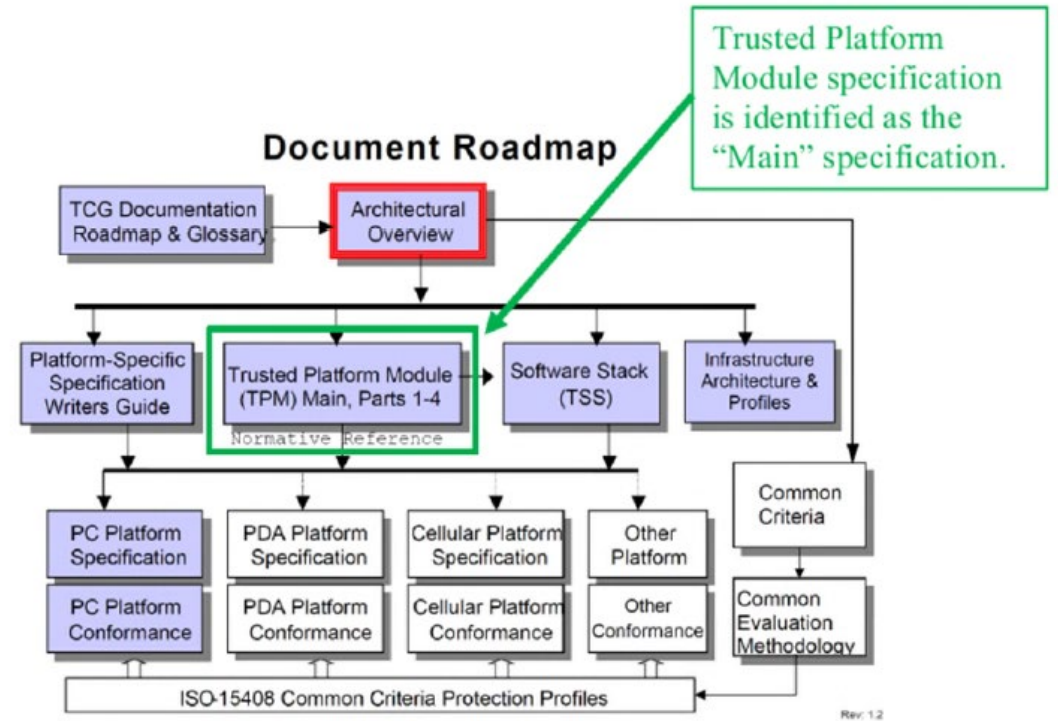


Reddy Declaration ¶ 87

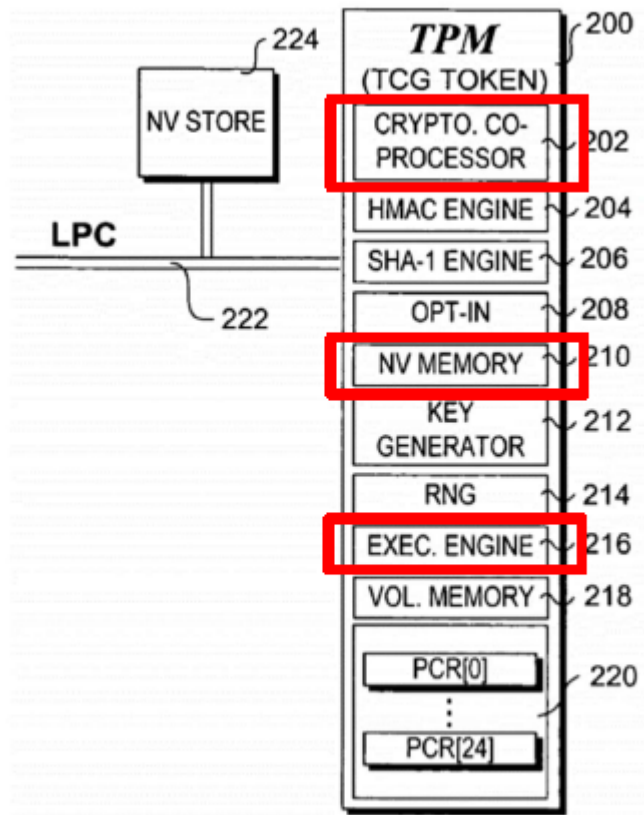


TCG Specification Architecture Overview at iv (annotated).

Shields Declaration ¶ XXX

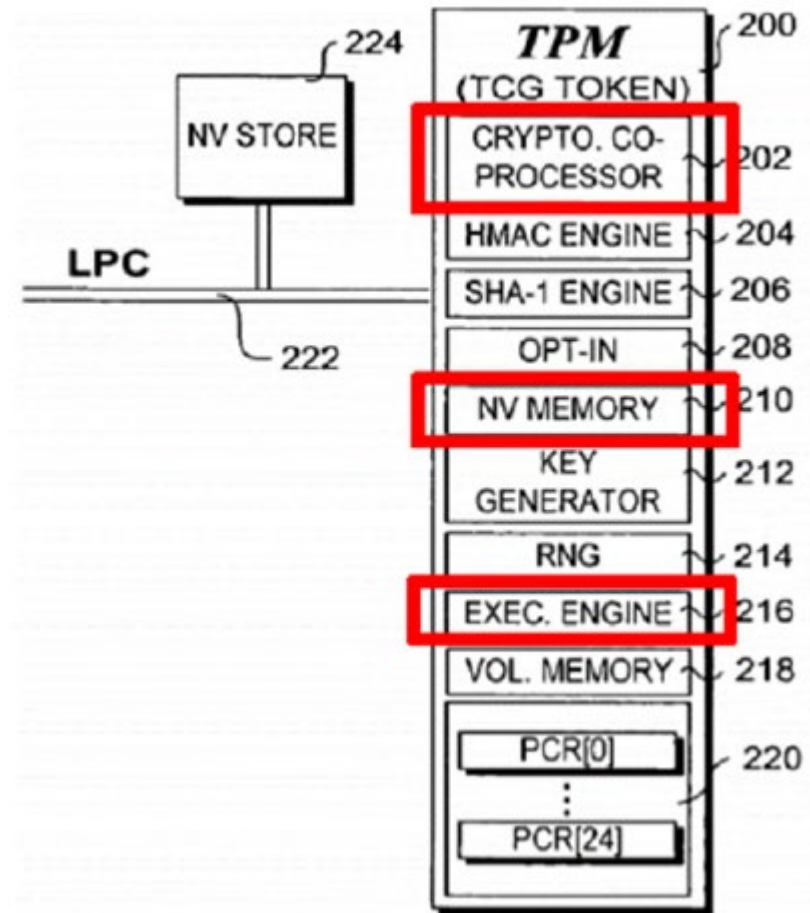


Reddy Declaration ¶ 88

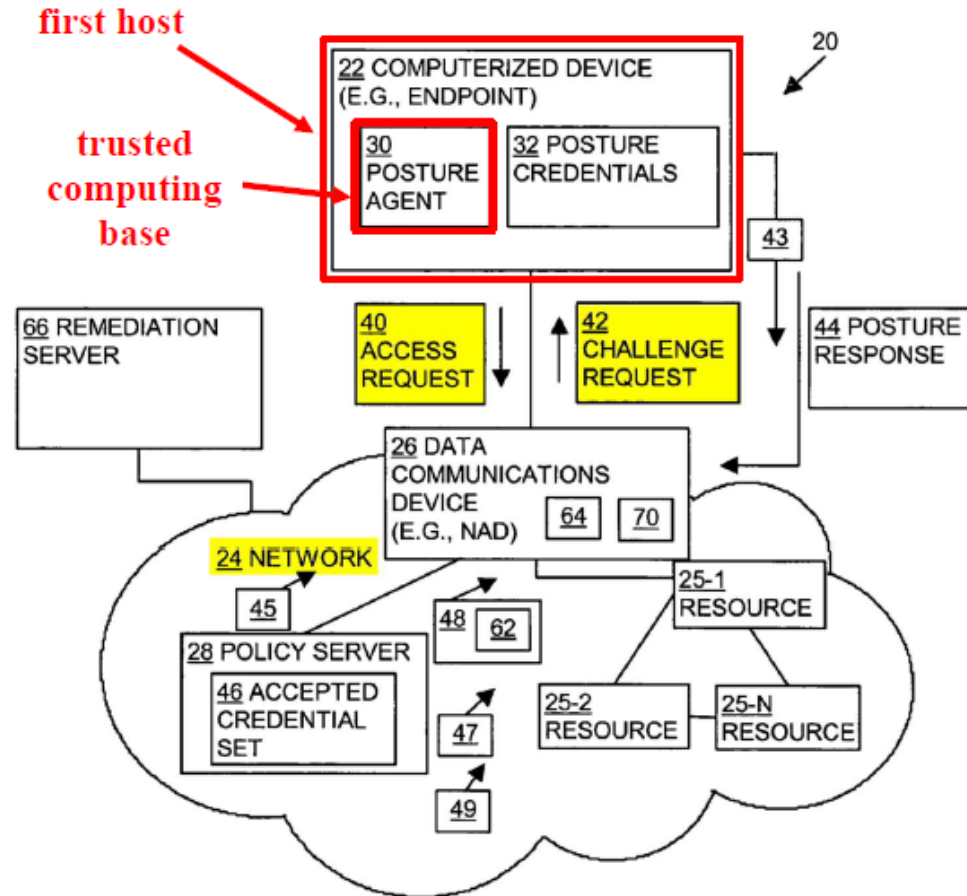


Ovadia at Fig. 2 (annotated).

Shields Declaration ¶ 86

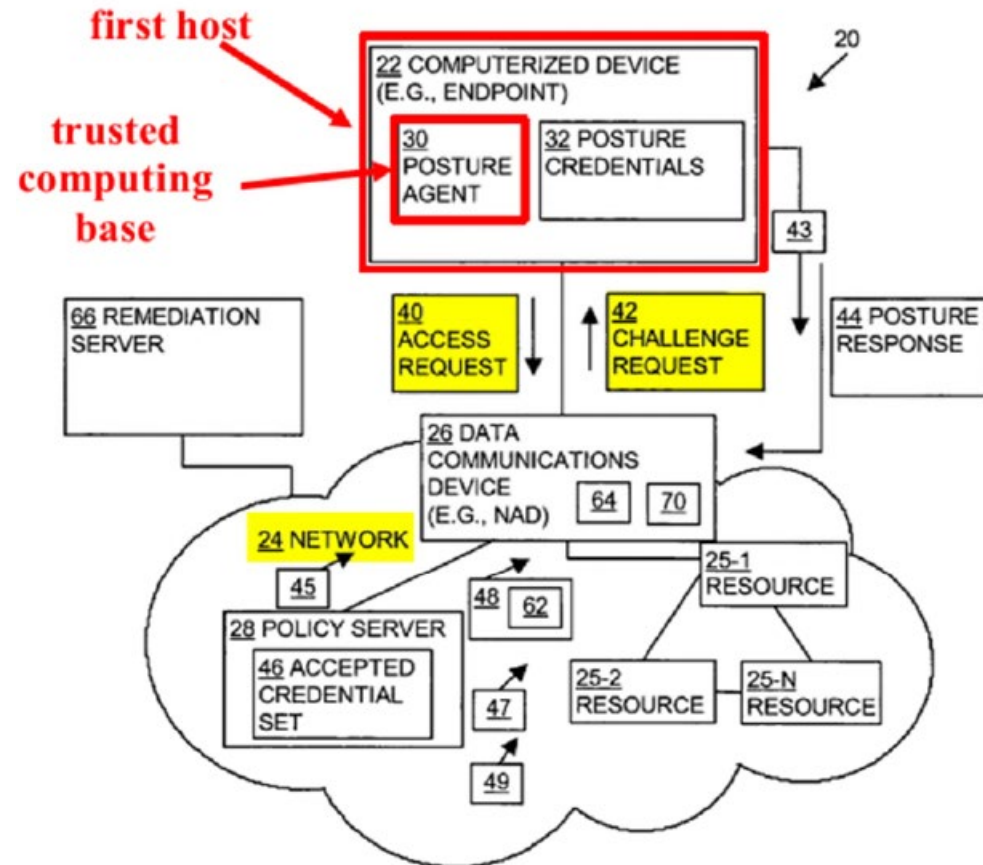


Reddy Declaration ¶ 91

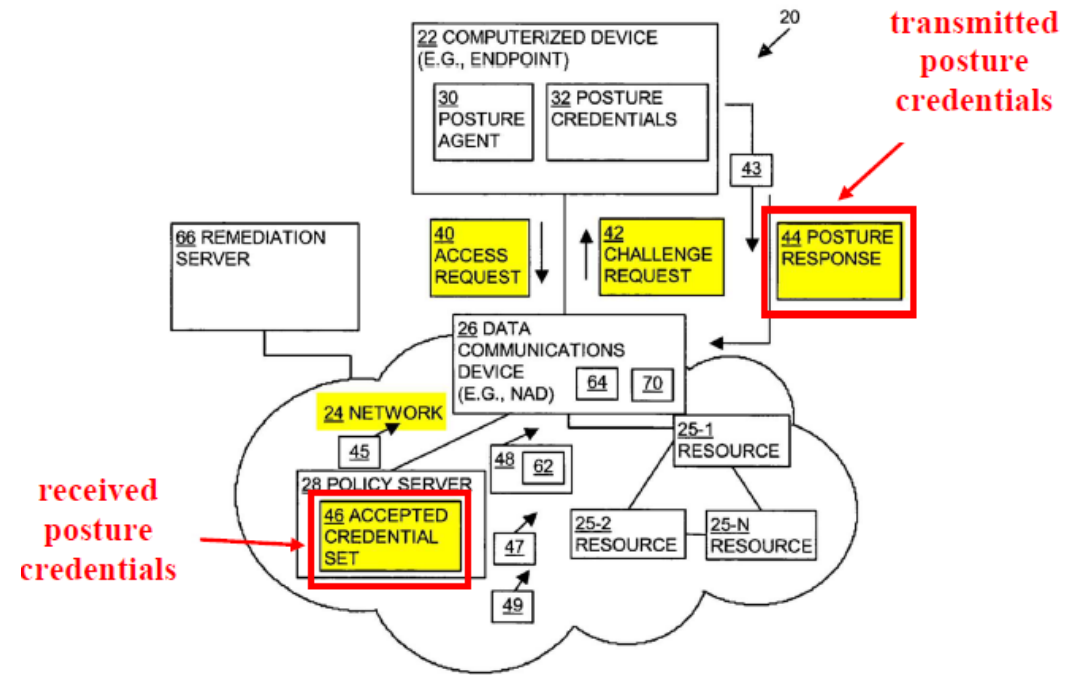


Glechauf at Fig. 1 (annotated).

Shields Declaration ¶ 87

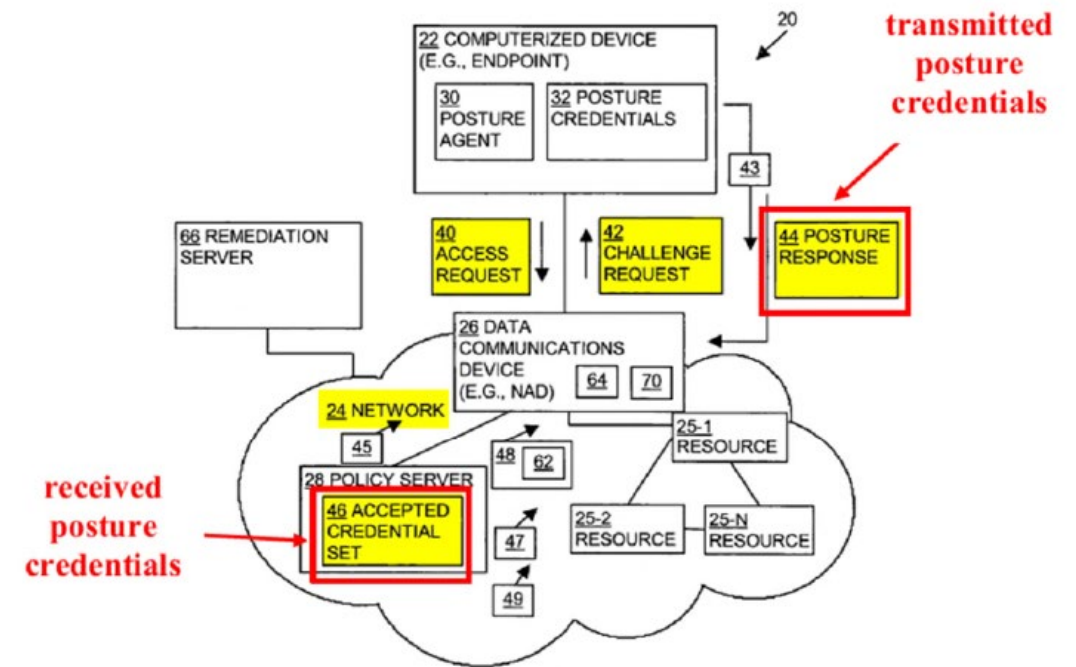


Reddy Declaration ¶ 98

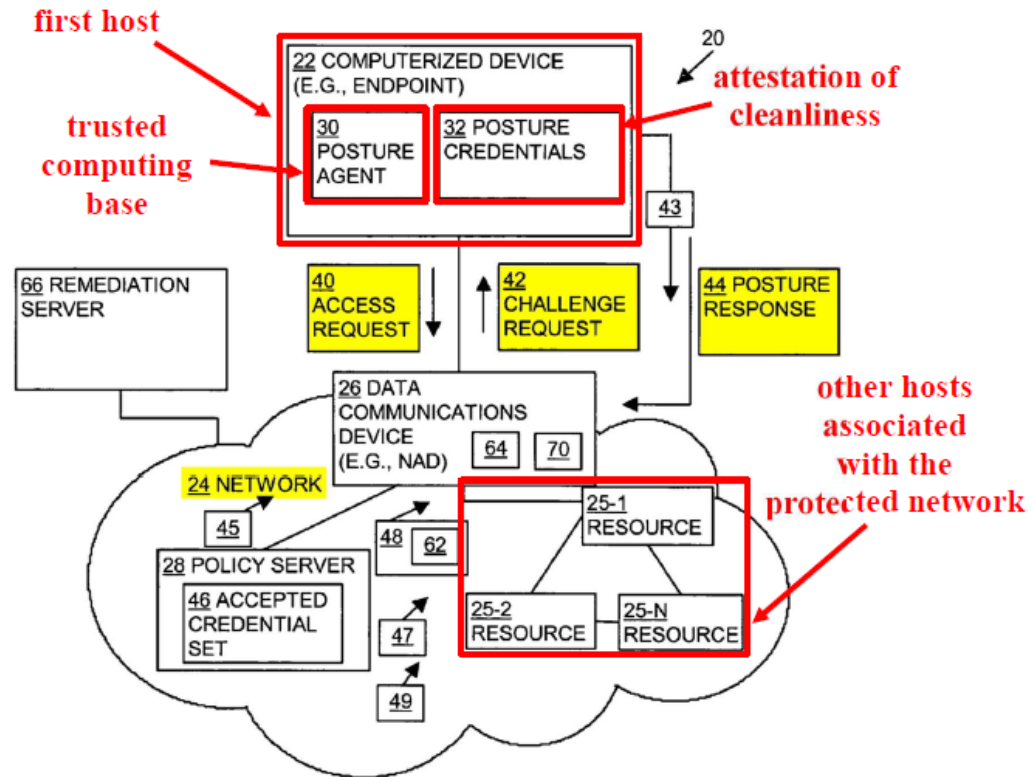


Gleichauf at Fig. 1 (annotated).

Shields Declaration ¶ 92

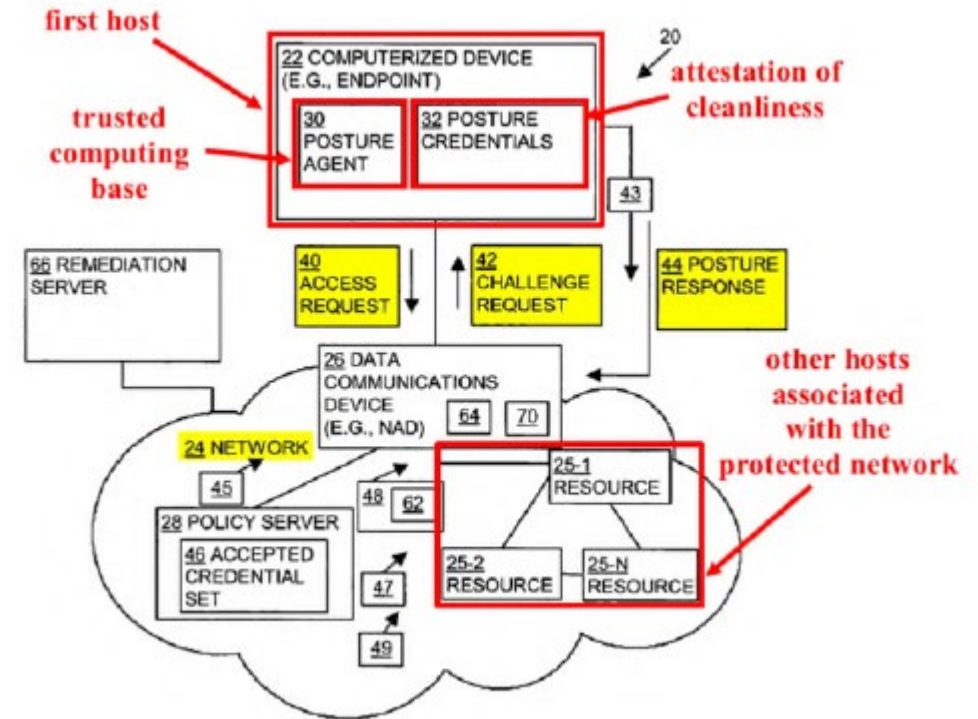


Reddy Declaration ¶ 124

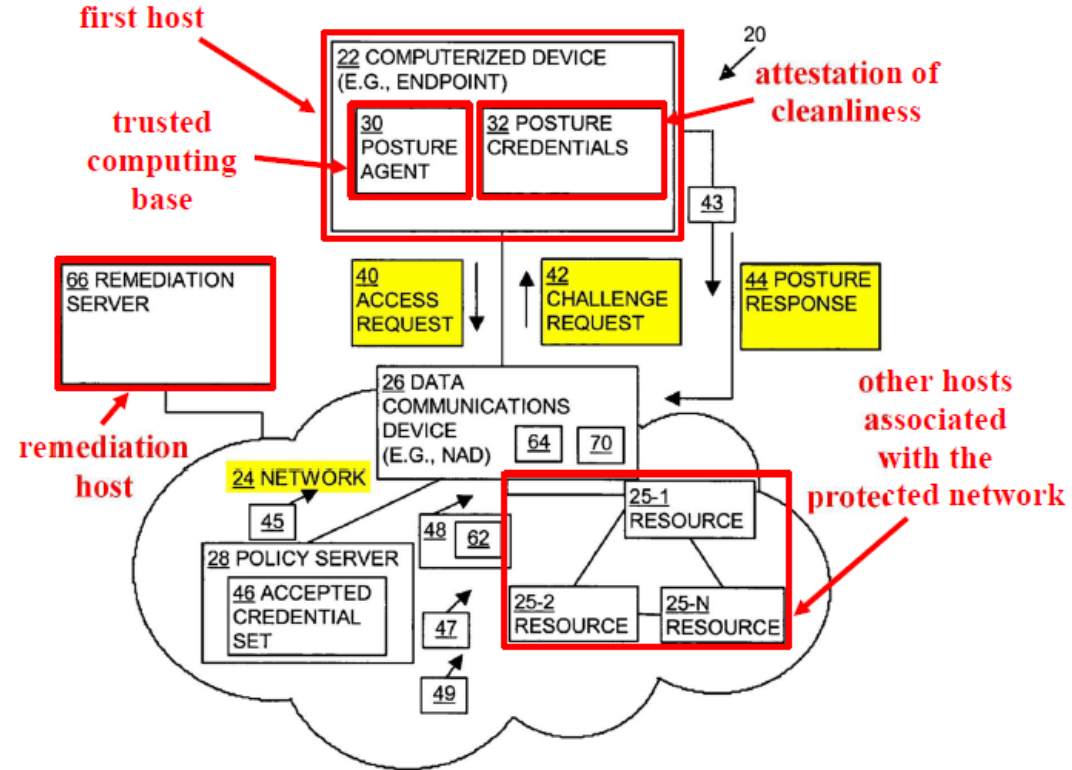


Gleichauf at Fig. 1 (annotated).

Shields Declaration ¶ 108

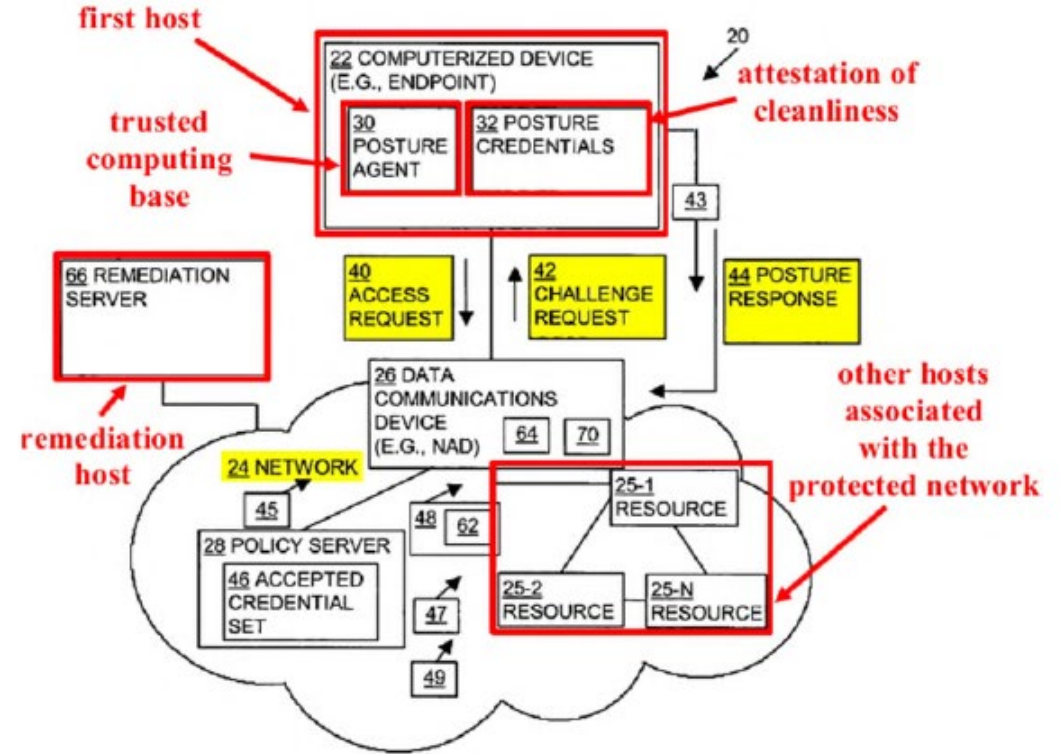


Reddy Declaration ¶ 142



Gleichauf at Fig. 1 (annotated).

Shields Declaration ¶ 118



Examples of Sentences Adding “In My Opinion” to Dr. Reddy’s Opinions

Reddy Declaration ¶ 56

56. A POSITA would have been motivated to take advantage of Ovadia’s use of a TPM—as described in the TCG “**platform-independent industry specification**”—because it would standardize Gleichauf’s posture credentials.

Shields Declaration ¶ 63

63. In my opinion, a POSITA would have been motivated to take advantage of Ovadia’s use of a trusted platform module—as described in the Trusted Computing Group “platform-independent industry specification”—because it would standardize Gleichauf’s posture credentials. EX1005, 4:32-35;

Reddy Declaration ¶ 60

60. A POSITA also would have been motivated to combine the teachings of Gleichauf and Ovadia because Ovadia provides additional details regarding implementation of Gleichauf's disclosed techniques.

Shields Declaration ¶ 66

66. In my opinion, a POSITA also would have been motivated to combine the teachings of Gleichauf and Ovadia because Ovadia provides additional details regarding implementation of Gleichauf's techniques.

Reddy Declaration ¶ 69

69. Serving a web page from a quarantine server would also give the user of the quarantined device the added option to elect to proceed with the recommended remediation or terminate the connection attempt.

Shields Declaration ¶ 72

72. In my opinion, serving a webpage from a quarantine server would also provide the quarantined device's user the option to proceed with the remediation or terminate the connection attempt.