

Credible Interoperability

Updated 02/07/02

Examples of how a TCPA subsystem can enhance security in B2B, B2E, and Web administration applications.

Example 1: Business to Business - B2B

The following scenario illustrates how a TCPA-compliant system adds to the authenticity, integrity and privacy of a B2B Public Key Infrastructure (PKI) deployment. In a vertical supplier/buyer e-Commerce model, TCPA capability enables a buyer to issue a challenge to the supplier platform to determine that it is a trusted system. This can be accomplished using an application that ensures that the transaction is correct to proceed. This challenge can be provided anonymously, in order to protect user privacy. For example, this capability can allow a TCPA-enabled PC user to browse anonymously, perhaps looking for the best prices among suppliers.

After deciding on a supplier, the buyer can challenge the server to determine that it is operating properly. The buyer can then utilize the TCPA subsystem to “digitally sign” the sales contract and send it to the seller. Digital signatures can provide assurance of the source of the data and that the received data is the same as the sent data. Digital signatures also prevent the data source from denying that the data was created by the source (a feature known as ‘non-repudiation’). If the TCPA-enabled system is digitally signing the contract, the identity used for the signature can be simultaneously reliable and anonymous. In this context, the TCPA-enabled system ensures that the transaction was not compromised by unauthorized hardware or software designed to spoof or hack the transaction. The result is a fully trusted transaction.

Example 2: Business to Environment - B2E

Today IT managers can have serious issues with authentication systems based on passwords, and rogue viruses are being introduced that can make difficult to be sure that the platform environment can be trusted. The TCPA system can be used to support an enterprise virtual private network, in order to enable access by employees located in remote sites. This scenario would employ 2-factor authentication devices (e.g., Smart Cards and/or biometrics) utilizing a TCPA-enabled system. This process, known as “remote attestation,” allows an application (the “challenger”) to trust a remote platform. This trust is built by obtaining “integrity metrics” in the remote platform, securely storing these metrics in the remote platform, and then ensuring that the reporting of the metrics from the remote platform is secure.

For example, before making content available to a remote user, it is likely that a provider will need to know that the remote platform is trustworthy. The provider’s platform (the “challenger”) queries the remote platform. During system boot, the challenged platform creates a series of cryptographic digests (integrity metrics) that represent the method used to build the software environment in the challenged platform. These digests are statistically unique indications of the platform environment, yet they will occur in all platforms with the same software environment.

When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering

and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy. If so, the challenger, in this case the service provider, can then deliver the content. The TCPA system reports the metrics and lets the challenger make the final decision regarding the trustworthiness of the remote platform. Based upon the reported integrity metrics, the challenger can determine if the platform is configured in a trusted state.

Example 3: Web administration

Today, an e-Business website doesn't really know that it can trust interactions with unknown parties. TCPA provides new capabilities to address this potentially costly issue. The following scenario illustrates how an e-Business website can trust interactions with unknown parties over the Internet by using a recognized and trusted third-party that can verify to the interactions are coming from a trusted platform. This is termed "anonymous authentication."

Here is how it works in a TCPA-compliant subsystem:

The user goes to a third-party Authenticated Anonymity Web site (AAWS), which could be provided by a PKI (Public Key Infrastructure) vendor, to request site verification. Using the TCPA Subsystem, the AAWS provides the user with certification credentials. These credentials assert that a trusted third party authenticates the user's platform and that the platform can be trusted in certain ways. The AAWS asserts that the platform is unique, but it will not disclose anything that can be traced back to the user. For the purposes of the transaction, the platform is reliable, and also anonymous. The user can store private data in a TCPA-compliant system and then select when to disclose the information. This improves existing applications that use security, including Web browsers with SSL and e-mail using S-MIME (Secure Multi-Purpose Internet Mail Extensions).