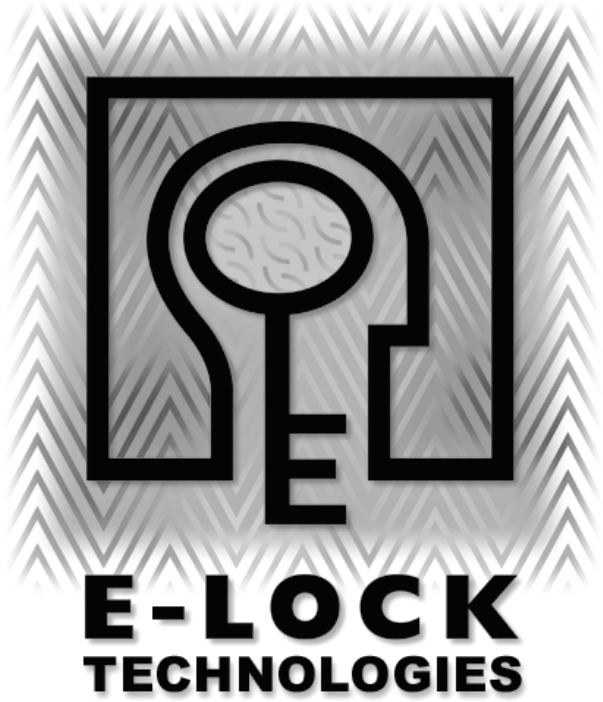
E-LOCK TECHNOLOGIES

Assuring e-Business



E-Lock ATS

PKI Technical Working Group

August 12, 1999

E-Lock ATS

- What is E-Lock ATS
- How E-Lock ATS Architecture can be used to Assure e-Business
- Case Study

E-LOCK TECHNOLOGIES

Assuring e-Business

What is E-Lock ATS?

- A modular security architecture for the development of e-Business products and services
- *Assured Transactions*™ (ATS) is a dynamic architecture, today it provides a reasonable level of legal defensibility, while the architecture will grow with the industry towards digital trust and non-repudiation.
- The criteria governing the ATS Architecture consists of Data Integrity, Authentication, Data Confidentiality, Time Stamping, Audit, Data Archive, and Chain of Custody
- The ATS Architecture is based on ATS Policies, Policy Management, and Policy Enforcement

What is Special about E-Lock ATS (1 of 2)

- *Centralized Policy Based Management.* E-Lock ATS provides centralized policy management and localized policy enforcement to manage and control the process of applying digital signatures and encrypting data for an organization.
- *Modular Security Architecture.* E-Lock ATS provides a modular, layered, security architecture to support *Assured Transactions*™ for e-Business.
- *Support for Multiple Security Frameworks and PKIs*. E-Lock ATS supports the Microsoft, Netscape, and Entrust security frameworks in addition to most certificate servers and Certificate Authorities. This allows E-Lock ATS to quickly and easily work with an organization's existing security and public key infrastructure.

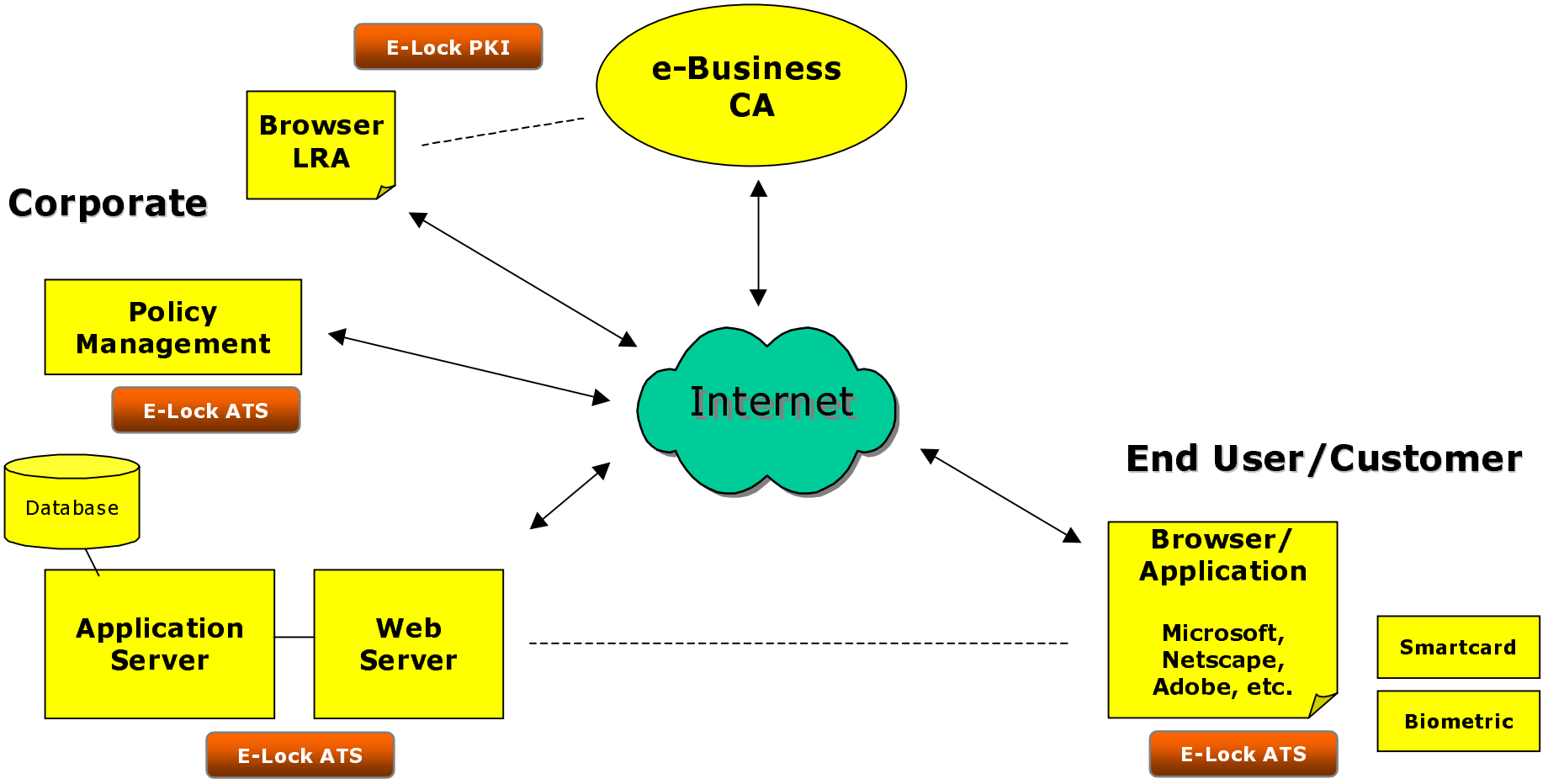
What is Special about E-Lock ATS (2 of 2)

- *Industry Standard.* E-lock ATS supports industry accepted standards and cryptographic algorithms like: HTML, XML, PKIX, X.509v3, PKCS#7, S/MIME, SSL, RSA, DSA, Diffie-Hellman, MD5, SHA1, RC2, RC4, RC5, DES, 3DES, etc.

E-LOCK TECHNOLOGIES

Assuring e-Business

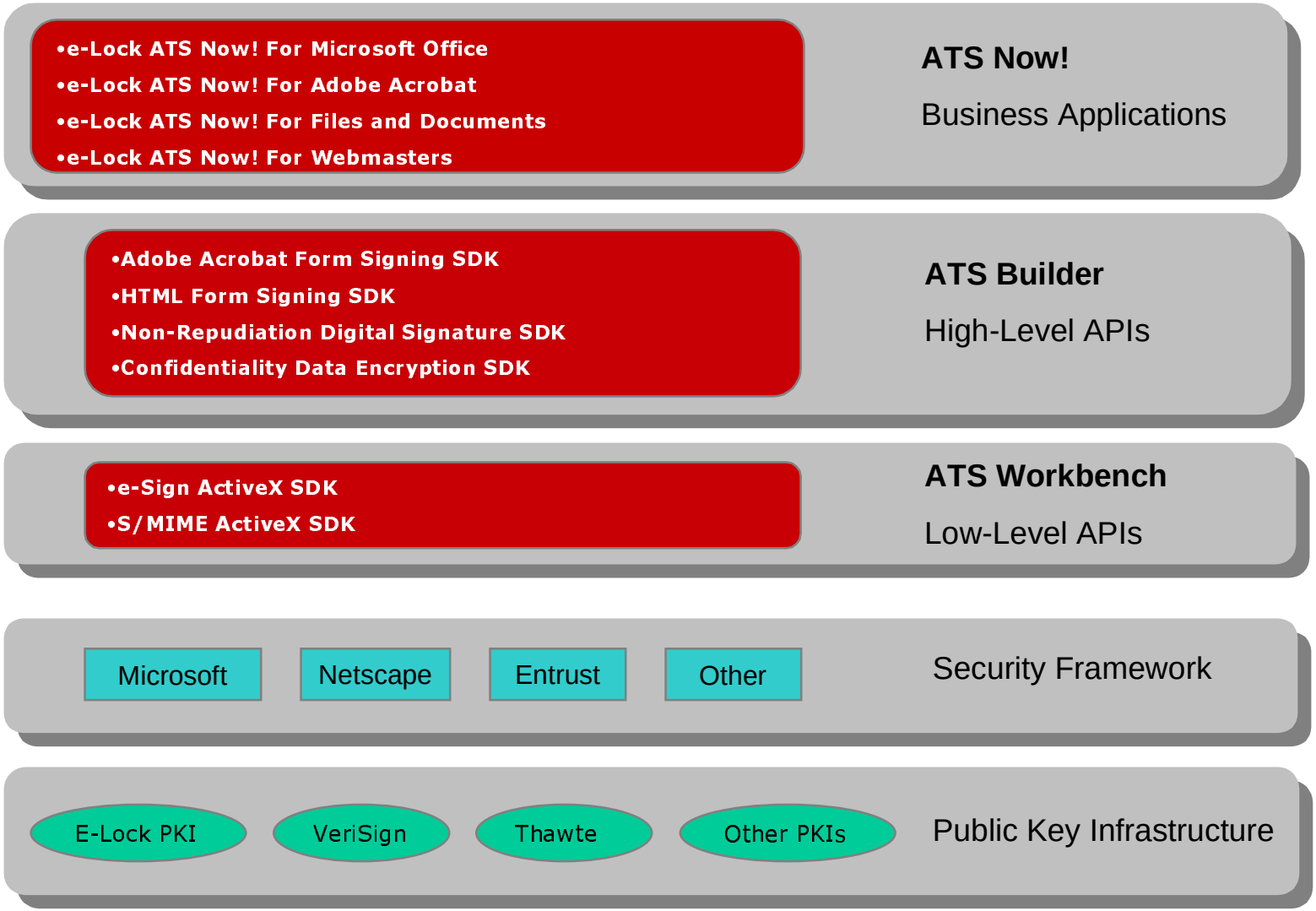
E-Lock ATS Client/Server Solution Architecture



E-LOCK TECHNOLOGIES

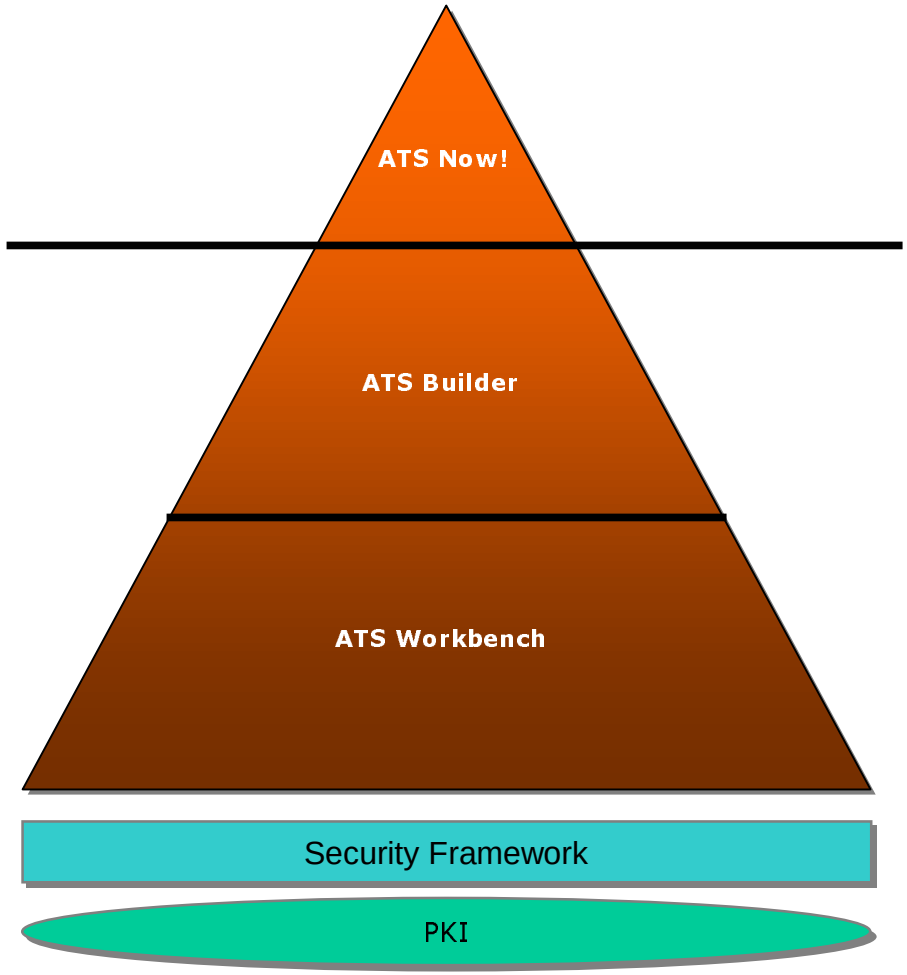
Assuring e-Business

E-Lock ATS Product Architecture



E-Lock Technologies

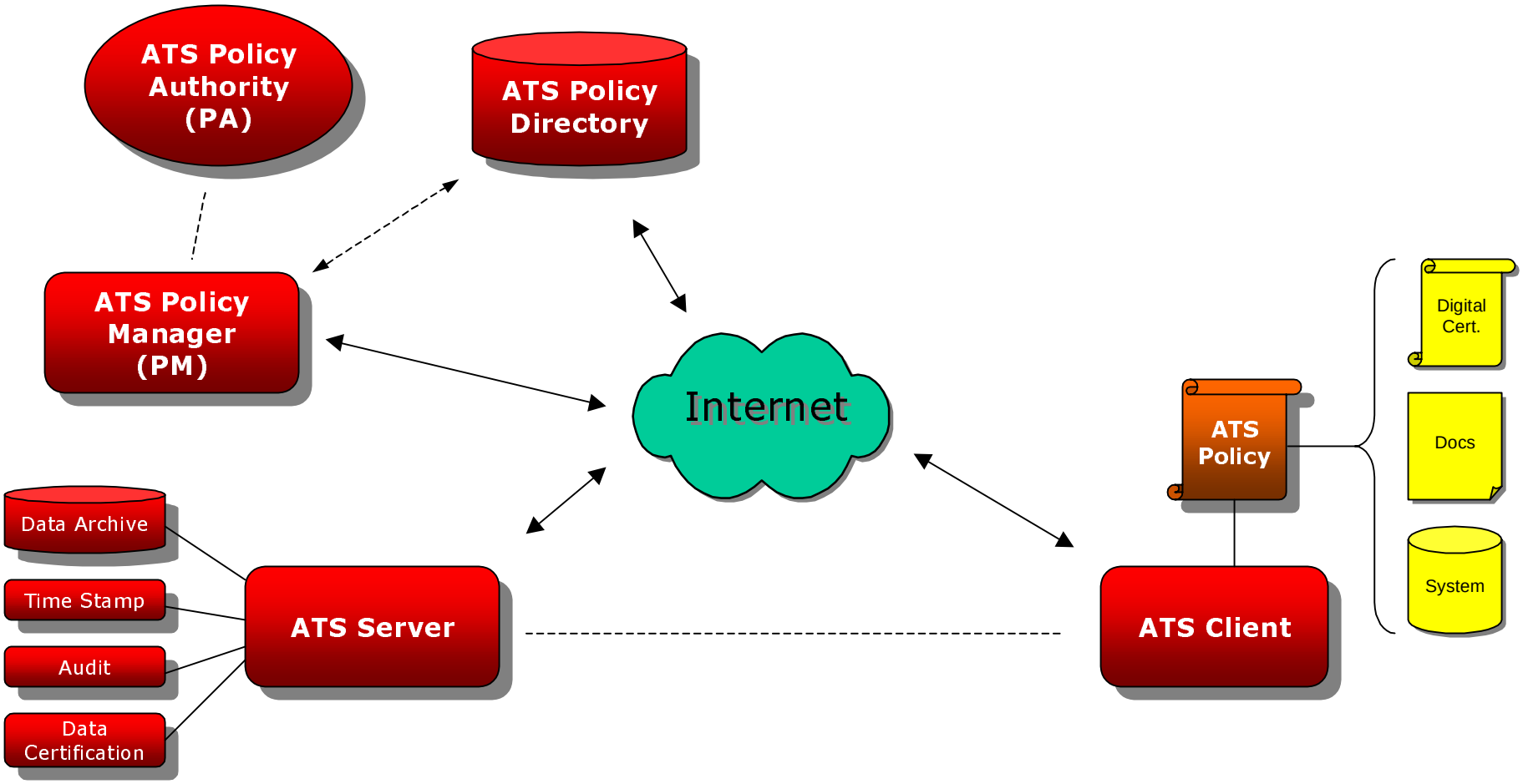
E-Lock ATS Now! Is just the "Tip" of the E-Lock ATS Architecture



E-LOCK TECHNOLOGIES

Assuring e-Business

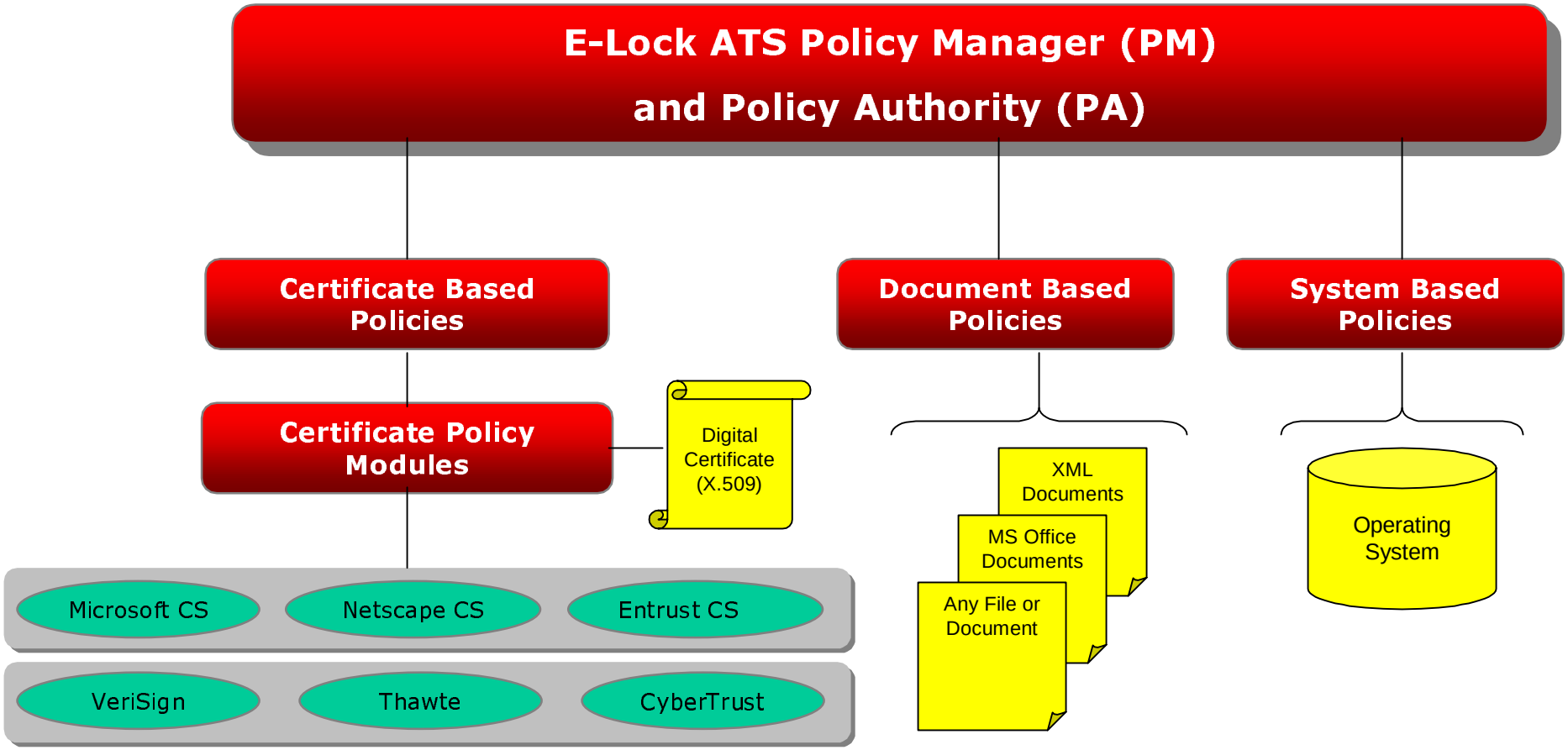
E-Lock ATS Architecture



E-LOCK TECHNOLOGIES

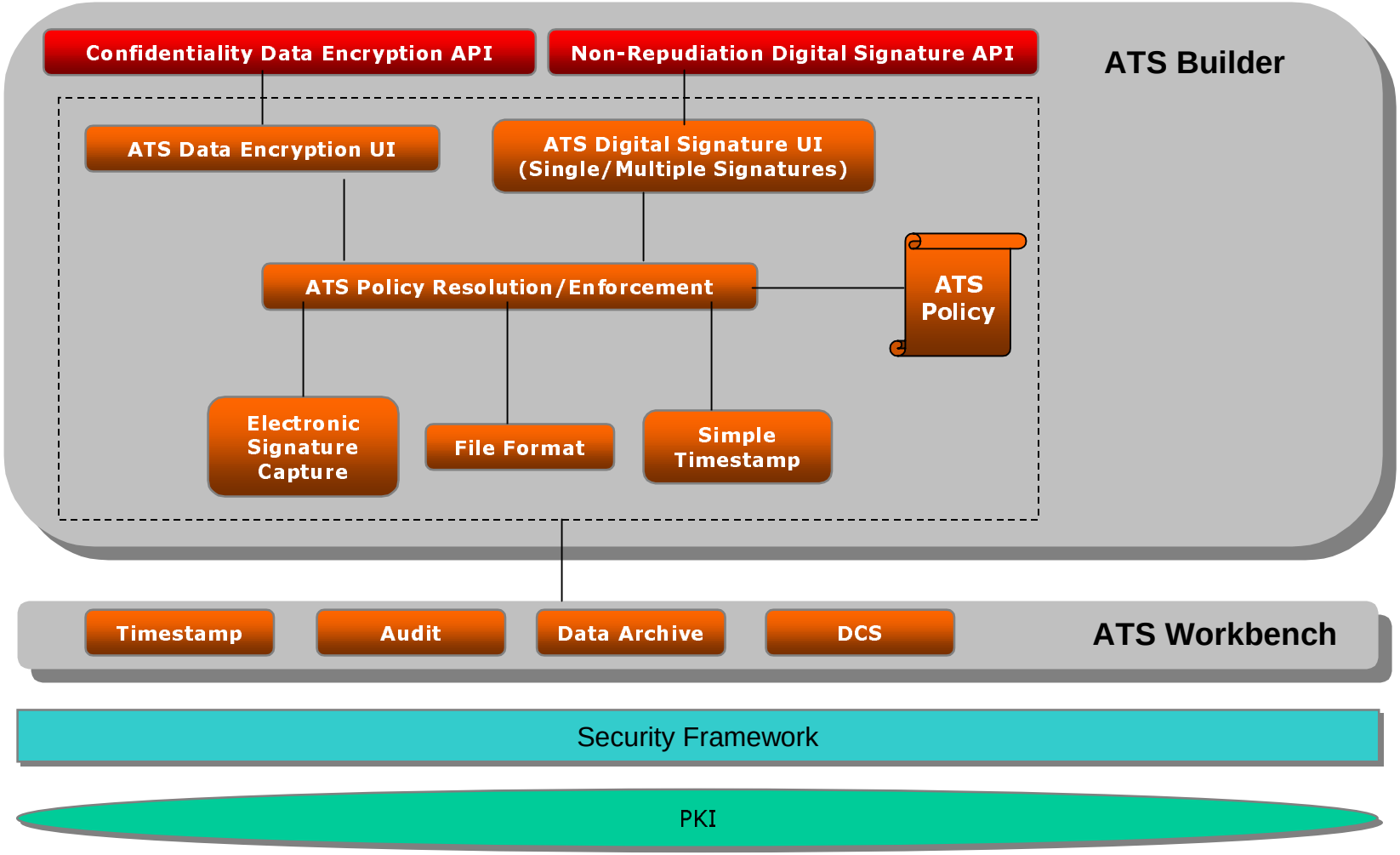
Assuring e-Business

E-Lock ATS Policy Manager and Policy Authority



E-LOCK TECHNOLOGIES

E-Lock ATS Policies and Policy Enforcement



E-LOCK TECHNOLOGIES

Assuring e-Business

E-Lock ATS Now!
Products

- *Completely Integrated with the E-Lock ATS Architecture.* Integration with the E-Lock ATS architecture allows full use of E-Lock ATS policies and policy enforcement to centrally manage and control the digital signature and data encryption process.
- ***E-Lock ATS Now! For Microsoft Office.*** Supports the Word and Excel applications. Embeds the ATS Digital Signature data directly into the Word or Excel document.
- ***E-Lock ATS Now! For Adobe Acrobat.*** Integrates the ATS Non-Repudiation Digital Signature architecture into the Adobe Acrobat 4.0 PDF file.
- ***E-Lock ATS Now! For Files and Documents.*** The digital signature and data encryption process is fully Integrated into the Microsoft Windows Explorer. Applying an E-Lock ATS digital signature or encrypting a file or document is as simple as right-clicking.
- ***E-Lock ATS Now! For Webmasters.*** Digitally Sign, Publish, and Verify HTML Content. Digitally signed content is automatically verified on the webserver before the content is sent to the web browser. The HTML document and any images on the HTML page are digitally signed by webmaster to maintain integrity and identity.

E-LOCK TECHNOLOGIES

Assuring e-Business

E-Lock ATS Builder

- *ATS Policies and Policy Enforcement.* The E-Lock ATS Builder brings the centrally managed and controlled ATS Policies and Policy Enforcement to E-Lock ATS enabled e-Business applications.
- *Multiple Signatures.* Any number of individuals can digitally sign a document as part of an approval or workflow process.
- *Electronic Signatures.* Supports a number of digitizing tablets to capture a handwritten signature image to place into a document.
- ***Non-repudiation Digital Signature SDK.*** This SDK provides developers access to the a complete functionality of applying an E-Lock ATS Digital Signature to their application data.
- ***Confidentiality Data Encryption SDK.*** This SDK provides developers complete access to the E-Lock ATS data encryption libraries.
- ***Adobe Acrobat form Signing SDK.*** This SDK provides client and server components for developers to integrate E-Lock ATS Digital Signatures into their Adobe Acrobat forms solutions.
- ***HTML Form Signing SDK.*** This SDK provides client and server components for developers to integrate E-Lock ATS Digital Signatures into their HTML forms based solutions for lesser-valued transactions.

E-Lock ATS Workbench

- *Low-Level components.* Supports a number of lower-level component functionalities to the E-Lock ATS architecture.
- ***E-Sign ActiveX SDK.*** This SDK provides a low level interface to basic cryptographic and certificate manipulation functions for Visual Basic, ASP, VBScript, etc. applications.
- ***S/MIME ActiveX/C/COM SDK.*** This SDK provides a complete interface to the S/MIME standard protocol. Developers can use this interface to build a number of secure messaging solutions for Visual Basic, ASP, VBScript, etc.
- ***Time Stamp SDK.*** This SDK provides a complete interface to the low-level time stamp client/server components in the E-Lock ATS architecture.
- ***Audit SDK.*** This SDK provides a complete interface to the low-level audit and event analysis client/server components in the E-Lock ATS architecture.
- ***Data Archive SDK.*** This SDK provides a complete interface to the low-level data archive components in the E-Lock ATS architecture.
- ***Data Certification SDK.*** This SDK provides a complete interface to the low-level data certification components in the E-Lock ATS architecture.

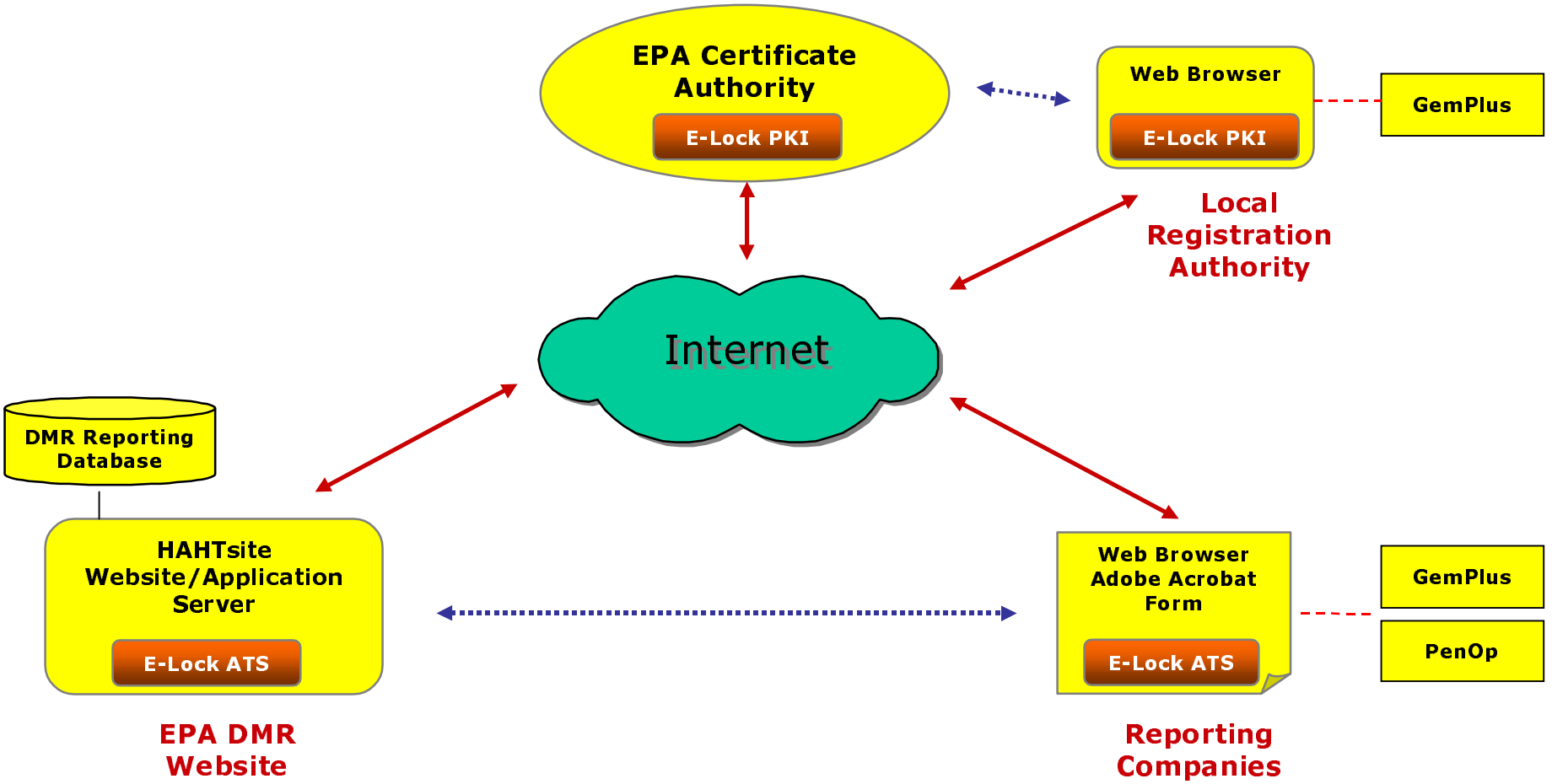
Example Solution That Uses E-Lock ATS Architecture

- **EPA DMR Pilot.** The goal of the EPA DMR Pilot is to provide digitally signed web-based forms that maintain a level of non-repudiation that is legally defensible.
- The E-Lock ATS Architecture has been deployed to provide a solution to submit digitally signed DMR forms which use:
  - Adobe Acrobat form signing (document of record)
  - GemPlus smartcards (private key protection)
  - PenOp (biometric evidence)

E-LOCK TECHNOLOGIES

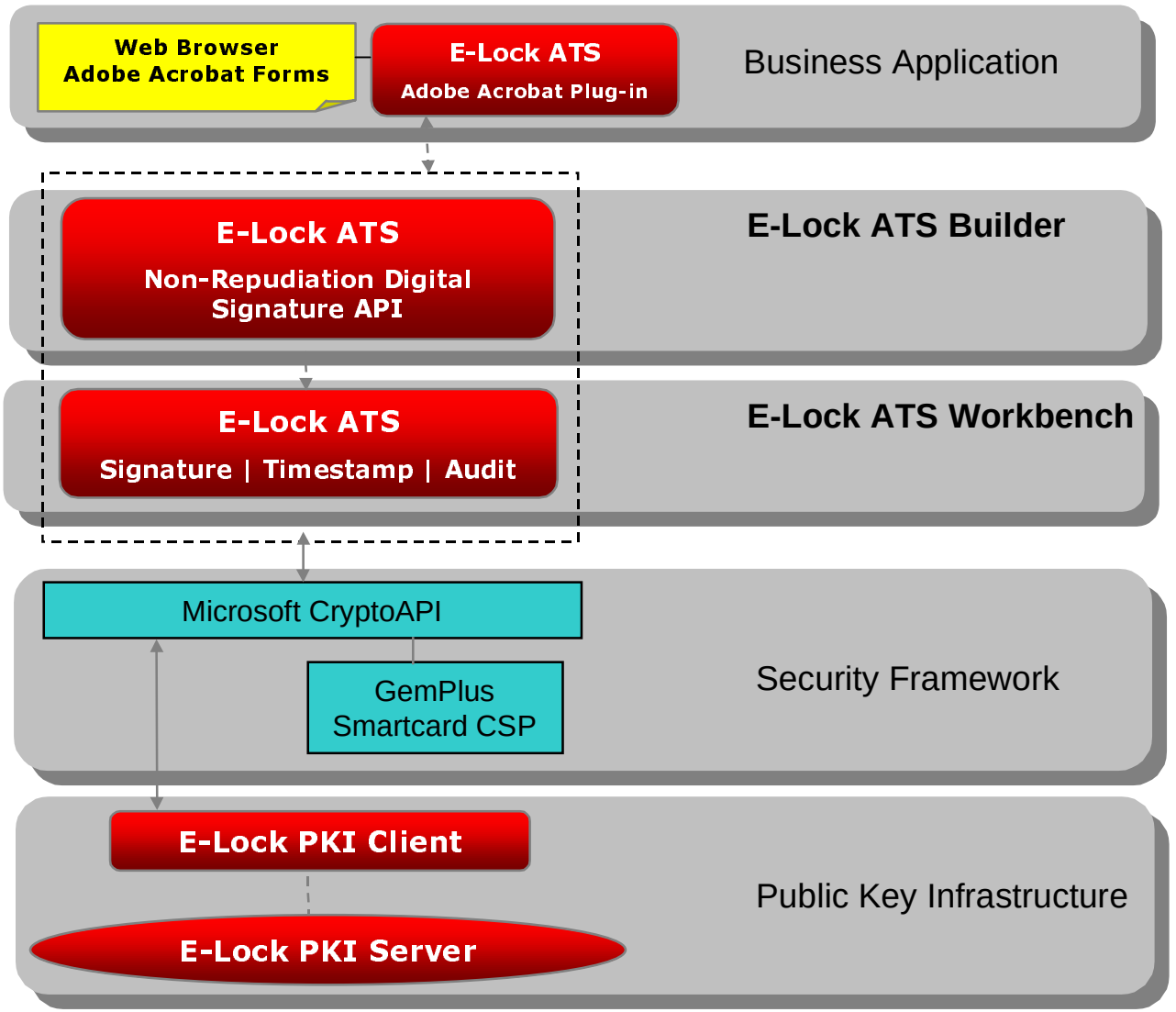
Assuring e-Business

EPA Pilot - Overview



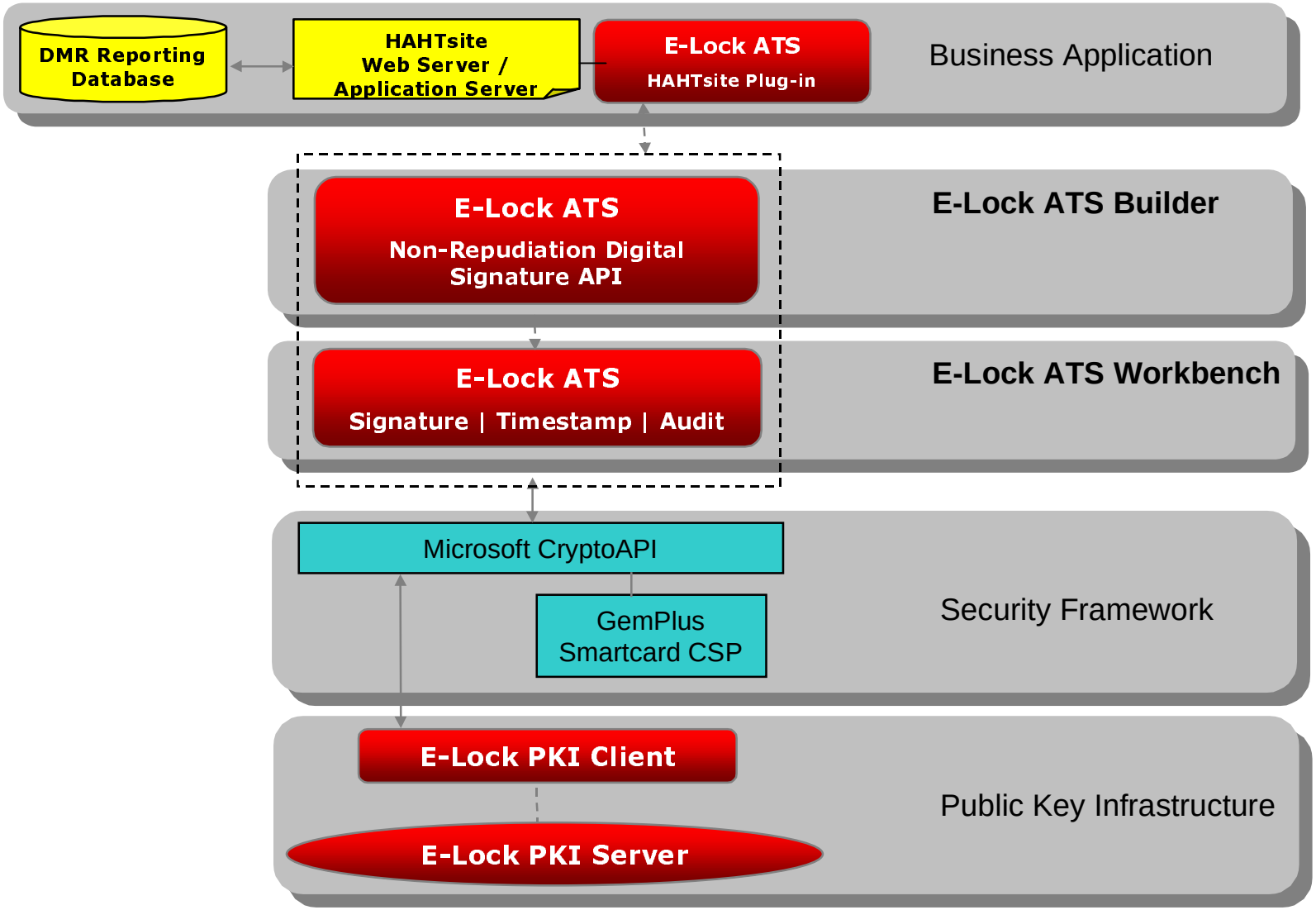
E-LOCK TECHNOLOGIES

EPA Pilot - Client Architecture



E-LOCK TECHNOLOGIES

EPA Pilot- Server Architecture



Summary

- *E-Lock ATS Architecture* is designed to Assure e-Business applications.
- *Centralized Policy Based Management and Local Policy Enforcement* is provided by E-Lock ATS to manage and control the process of applying digital signatures and encrypting data for an organization's e-Business processes.
- *Business Applications* need E-Lock ATS Digital Signature technology to make them *e-Business* applications.

Questions

E-LOCK TECHNOLOGIES

www.elock.com