



POINT OF VIEW

---

## Securing RFID Data for the Supply Chain



Where it all comes together.™



## Introduction

---

Now more than ever, enterprises operate in a global economy. Whereas 10 or 20 years ago manufacturing and supply operations were in close proximity, today they are dispersed throughout the world. Global sourcing and other changes in operations allow companies to focus on the high-value aspects of their business, but also drive the need for an operating model that can effectively span a distributed, multi-enterprise supply chain.

The Electronic Product Code™ (EPC) is emerging as one technology utilizing advanced sensory systems (e.g., Radio Frequency Identification [RFID]) to enable efficiency and accuracy of business operations throughout the extended supply chain. Through sharing data about supply and demand, enterprises can sense changes in the supply chain as they occur in near real time. Leveraging a standards-based IP network is the most efficient way to share this information; however, its use introduces concerns over data security and integrity. Therefore, an intelligent security framework is recommended to ensure that information is distributed or accessed as outlined by the security policies defined by the enterprise and extended to the entire supply chain.

Fortunately, the paradigm of conducting critical business on the Internet is well established and understood. Every significant business in the world conducts some level of business online. Enabling this is a variety of existing, proven technologies that address common security challenges for conducting trusted commerce and communication across today's complex global networks.

This paper outlines security concerns around sharing RFID and EPC supply chain information across an IP-based infrastructure and highlights existing security technologies to address them. It does not cover all RFID-related security issues, but focuses on the appropriate security measures for beginning the exploration of data sharing. As the supply chain community begins this exploration, security need not be perceived as a barrier to pilots that target network-based processes.

## The Security Challenge

---

As companies continue to expand business processes with trading partners, they are beginning to share critical supply chain data over the Internet. The importance and sensitive nature of this information forces security concerns to be taken seriously at the onset of any RFID pilot or proof of concept. Companies need trusted and proven technologies that provide security and are as flexible and adaptable as their supply chains. Additionally, companies should look for standards-based solutions to ensure that their technology choices have long-term market viability and support.

Security must not disrupt the supply chain or cause undue burden on and complexity to existing business processes. Security technologies must be scalable and reliable in order to support a supply chain through which trillions of dollars of goods move. Security cannot disrupt the supply chain without severe downstream effects.



## AUTHENTICATION SUMMARY

- Answers the question: Who is this organization or individual?
- Function: Provides the ability to reliably establish the identity of the communicating party (trading partner or individual).
- Example technology implementations: X.509 digital certificates, username and passwords, smart cards, user authentication tokens.

There are three major challenges that any security framework must address:

- Authentication
- Data protection
- Access control

### + Authentication

Authentication is the process of verifying that a peer entity in a communication is who or what it says it is. Authentication is a critical element of any security framework. Sending sensitive information across a network without knowing who is on the other end could create serious risks, including exposure of sensitive supply and demand information to competitors and the risk of regulatory liabilities arising from improper disclosure of information.

We use a variety of identification methods in our day-to-day life. For example, most companies require customers to present a driver's license or other form of identification when writing a check. Some banks are starting to use biometric thumbprints to authenticate the identity of customers.

Today, companies also need to identify and authenticate trading partners. Trusted trading relationships require mutual authentication of both the sender and receiver of critical supply chain information. It is unreasonable to expect companies to create a separate authentication process for every trading partner relationship. Without a repeatable, automated way of authenticating the identity of organizations, individuals, and devices, the business data and utility of any technology will be undercut. The effect will be an underutilized implementation that does not maximize the capabilities of the trading network.

As an example of the importance of authentication, imagine a supply chain transaction between two imaginary companies, ACME and RETAIL Co. RETAIL Co. receives an order from ACME of 1,000 items at its regional distribution center. To confirm the authenticity of the product, RETAIL Co. initiates a search on the EPCglobal Network™ to determine specifics of the shipment received. Since they initiated the shipment, ACME's systems are contacted with the authentication query. But how can ACME be sure the query actually came from RETAIL Co. and not from a competitor? Providing any information to a competitor about RETAIL Co.'s orders would put RETAIL Co. at a disadvantage and potentially expose ACME to liability.

To protect themselves against unauthenticated and unauthorized queries, ACME and RETAIL Co. need to be able to authenticate. After authentication, they will need to ensure that the parties make authorization checks corresponding to queries. Please see the Access Control section for more information.

Authentication usually starts with identification—one communication partner starts a conversation with another and claims an identity. After the first entity identifies itself, the entity at the other end of the conversation will usually want to verify the first entity's claimed identity. Depending on the nature of the conversation, the initiator of the conversation may also want to identify the party at the other end of the line and authenticate its identity; when this happens, we say that the entities mutually authenticate one another.

A variety of authentication options are available in today's information security technology market. Some companies employ PKI technology to assign and manage verifiable virtual identities. PKI technology has several advantages, including a well-defined trust model and



## DATA PROTECTION SUMMARY

- Answers the question: How do I know that no other parties are intercepting my communication with my trading partner? How can I ensure that the data sent has not been tampered with prior to transmission?
- Function: Provides the ability to scramble the transmission of the data between two trading partners so the data cannot be intercepted in transit.
- Example technology: Encryption, PKI, SSL, 128-bit crypto algorithms.

the ability to make users accountable for their actions. Existing Web security protocols support PKI-based authentication. Web applications, including browsers, Web servers, and Web application servers, utilize this PKI support and provide users and enterprises with a rich set of tools for managing identities.

RFID implementations rely heavily on collecting data with limited human interaction, so a critical element of authentication in next-generation supply chains will be RFID reader authentication. An example of device authentication in use today is cable modems. When cable modems are manufactured, they are imbedded with cryptographic keys and an associated digital certificate that is used to cryptographically verify the identity of the modem. This enables the cable operators to provision and configure customers securely and assures authorized access to the cable broadcasts by authenticated cable modems.

### + Data Protection

A second critical element of a security framework is data protection. Data protection ensures that information cannot be intercepted or modified by unauthorized parties while it is in transit across networks or resident on storage media. Typically this is achieved by encrypting the transmission before it is sent, and decrypting it after it is received.

Data integrity ensures data has not been changed, destroyed, or lost in an unauthorized or accidental manner. It usually implies that there are well-regulated procedures for creating, modifying, and deleting data. Data integrity can be ensured at two levels—confidentiality and integrity.

- **Confidentiality**—Data confidentiality provided by the transport protocol layer (SSL or TLS) ensures that the data is visible only to the authorized sending and receiving parties. This ensures that communication is not compromised in transit. Such transport layer security is only effective while the transport session is active. This technology only ensures end-to-end confidentiality of the data while in transmission.
- **Integrity**—The purpose of message integrity is to ensure that data has not been altered in transit and is from a verifiable authenticated source. Data can be secured even when not in transit, such as before processing is completed.

As an example, we'll look at how encryption provides data integrity in the earlier described transaction between ACME and RETAIL Co. Assume that the product authenticity query comes into ACME's systems, and that ACME can authenticate that the request has come from RETAIL Co. ACME's systems will then transmit the requested data to RETAIL Co. over the Internet. Through the authentication process, ACME can be sure it is not sending information to an unauthorized entity, but how can both parties be sure that the data will not be intercepted during transmission?

What ACME and RETAIL Co. need is a mechanism which helps ensure that messages don't get changed, accidentally or maliciously, during transmission, and which also helps to ensure that only they can read the contents of the messages they exchange.

Data integrity is provided using cryptographic mechanisms including message authentication codes and digital signatures. A technology used on most major e-commerce Web sites and business exchanges is 128-bit encryption. The 128-bit encryption technology is a marked enhancement over 40-bit encryption and is 300 septillion (300 with 24 zeros) times stronger. VeriSign estimates that a hacker with access to a high-end home system would require a trillion years to break a 128-bit encrypted transaction. The good news is that this well-understood technology can be implemented today in pilots using the EPCglobal Network, where critical supply chain data is traversing the Internet.



## ACCESS CONTROL SUMMARY

- Answers the question: What data is this authenticated partner or user allowed to see?
- Function: Provides the ability to control access to data and permissions for users and limits what they can do with the data.
- Example technology: Policy server, access control software, identity management software

### + Access Control

The third critical element of a security framework is access control. Access control ensures that security-sensitive tasks are performed only by properly authenticated individuals who have also been authorized to perform them. When deployed properly, it limits or grants access to information based on predetermined rules.

Access Control mechanisms have four major functions:

- Using credentials provided by authentication mechanisms to determine the identities of each party who tries to perform an operation
- Consulting an identity management service to determine the roles or other authorities granted to an identified party
- Determining the sensitivity of the operation requested by an identified party
- Consulting an access management service, which evaluates authorization rules defined by the business to determine whether the identified party's credentials, roles, and authorities allow that party to perform the requested operation, in light of its sensitivity

Using the example of ACME and RETAIL Co., the two entities have authenticated one another as part of their transaction. RETAIL Co. is now able to ask questions of the system and get responses. However, there must be controls in place to ensure they don't receive access to information about a competitor that ACME may have in its systems. Additionally, there may be requirements for rules that ensure that information available to RETAIL Co. is segmented based on the role of the requesting individual. Clearly, ACME and RETAIL Co. both have an interest in ensuring that their rules are enforced by their supply chain systems.

Because different parties in a supply chain are likely to have different user management and authentication requirements, each party still needs to be able to identify, authenticate, and authorize all other parties' users. It is important that access control systems be able to support multiple authentication mechanisms by consuming and understanding the credentials they generate. Standards like Security Assertions Markup Language (SAML) and Web Services Security Language (WS-Security) facilitate this type of interoperability.

Because one organization (e.g., ACME) should not be forced to bear the burden of administering accounts for users from other organizations (e.g., RETAIL Co.), it is important for authorization systems to support delegation of administrative authority. In our example, an ACME administrator should be able to delegate to a RETAIL Co. administrator the ability to add users to the "RETAIL Co. Purchasing Officer" role and to remove users from that role.

Access control software should support multiple authentication mechanisms, allowing users to log in using a user ID and password, digital certificates, shared secrets, secure tokens, etc. There should be support for auditing security events such as authentication and authorization events, including both successful and unsuccessful access to resources, password changes, and administration or management events.

An important aspect of an effective access control solution is adherence to standards. A standards-based solution can accommodate other key application providers. Additionally, access control solutions should be modular to allow for separation of security code from application code. This translates to improved time to market and return on investment for

customers as they can change application code without affecting security code and vice versa. Advanced access control solutions should integrate with federated identity management to provide solutions that work in a cross-enterprise environment, which requires cross-enterprise identity mapping and provisioning, trust management, and trust brokering.

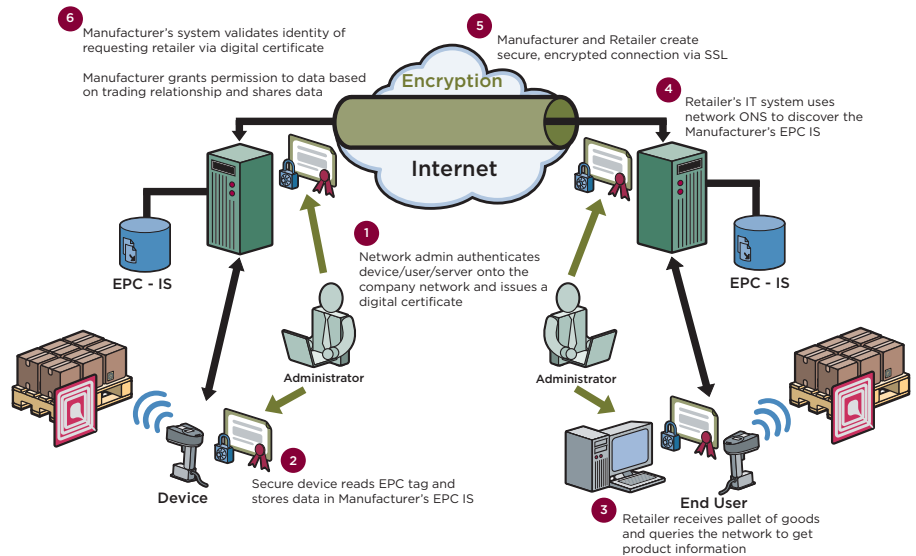
## Conclusion

As integration of RFID into the supply chain moves past compliance phase, many projects are exploring the benefits of RFID in driving operational efficiency within the warehouses where it is deployed. But an increasing number of progressive companies are recognizing that the real value of RFID is tied to the challenges of visibility beyond the warehouse and the enterprise's four walls. Thus, multi-enterprise processes become the path to greater ROI for RFID, and drive the need for data sharing across trading partner boundaries.

Concerns over the security and integrity of data being shared over the Internet through the EPCglobal Network need not be a barrier to pilot or production deployments that involve multiple enterprises. Proven security technologies can satisfy the core needs around data security and integrity, specifically authentication of trading partners, control of access to sensitive data between trading relationships, and encryption of data in transmission.

The chart below depicts how these technologies can work in concert to provide a simple, multi-enterprise exchange of data across the Internet, and highlights the role of each technology in protecting sensitive data.

### Chart



This chart depicts an end-to-end query between a Manufacturer and a Retailer, highlighting the use of current technologies to authenticate the trading partners, control access to certain information, and encrypt data before it is transmitted across the Internet.



VeriSign, a leader in enabling secure commerce and communication across today's complex global networks, is helping companies employ a secure solution architecture to address high-value supply chain process. By integrating standards-based security solutions and by leveraging the data sharing capabilities of the EPCglobal Network, leading companies can drive shorter development time for solutions and ensure interoperability of these solutions with suppliers and retailers to create valuable multi-enterprise process development.

Many companies have begun their exploration of the benefits of sharing RFID-generated data with their trading partners. If you are interested in learning more about how VeriSign can help you target high-value processes that benefit from the enhanced visibility created by secure data sharing, visit [www.verisign.com/epc](http://www.verisign.com/epc).

#### **+ About VeriSign**

VeriSign Inc. operates intelligent infrastructure services that enable people and businesses to find, connect, secure, and transact across today's complex, global networks. Everyday, we enable over 14 billion Internet interactions, 3 billion telephony interactions, and \$100 million of e-commerce. We also provide the services that help over 3,000 enterprises and 400,000 Web sites to operate securely, reliably, and efficiently.

In January 2004, VeriSign was selected by EPCglobal to manage the Root ONS registry for the EPCglobal Network. This directory facilitates next generation supply chain processes by providing real-time access to sensory-level data for individual products across a network of trading relationships using the Electronic Product Code (EPC). In September 2004, VeriSign announced the availability of the EPC Starter Service, a bundle of network services that helps companies target multi-enterprise process opportunities.

In 2005, we look forward to sharing our point of view and additional announcements that support network-centric business models and help enterprises pragmatically pursue business process improvement opportunities. We will share a structured ROI-driven roadmap and solution architecture with our customers that make it easy to focus efforts on high-value areas of the business. We remain convinced that RFID, in the context of next-generation, net-centric business models, presents an exciting opportunity to extend the reach and accuracy of tomorrow's market leaders.

#### **+ To Learn More**

Visit [www.verisign.com/epc](http://www.verisign.com/epc) or contact us directly at [epc@verisign.com](mailto:epc@verisign.com).

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**