

# Applied PKI – Lesson 1

*The following represents an attempt to describe how Public Key Infrastructure (PKI) can be applied to common business processes. As a sample process the purchase order process has been selected, mainly due to fact that most people who have worked in reasonable large organizations, in some way have been involved in the not always so simple procedures associated with the purchasing of goods or services. In addition, the purchase order process is also fairly universal featuring key elements such as authorization, collaboration, and archiving, as well as usually being a multi-organization activity (e.g. buyer and seller). This document is one of a series of documents showing different approaches to applying PKI, but outside of its original heritage, secure person-to-person e-mail and login.*

## **What is a Purchasing System?**

Before digging too far it is important to have some basic understanding of how “e-purchasing” is currently handled. In the center there is usually a purchasing server keeping track of the entire purchasing process and aiding purchasers in supplier and product selections as well as linking purchases to appropriate cost centers. Outgoing orders are archived in the purchasing system which also matches received invoices and deliveries with outstanding orders. By centralizing information, such a system is able to anytime give a consolidated view of most purchasing activities.

## **Putting the enterprise PKI to work**

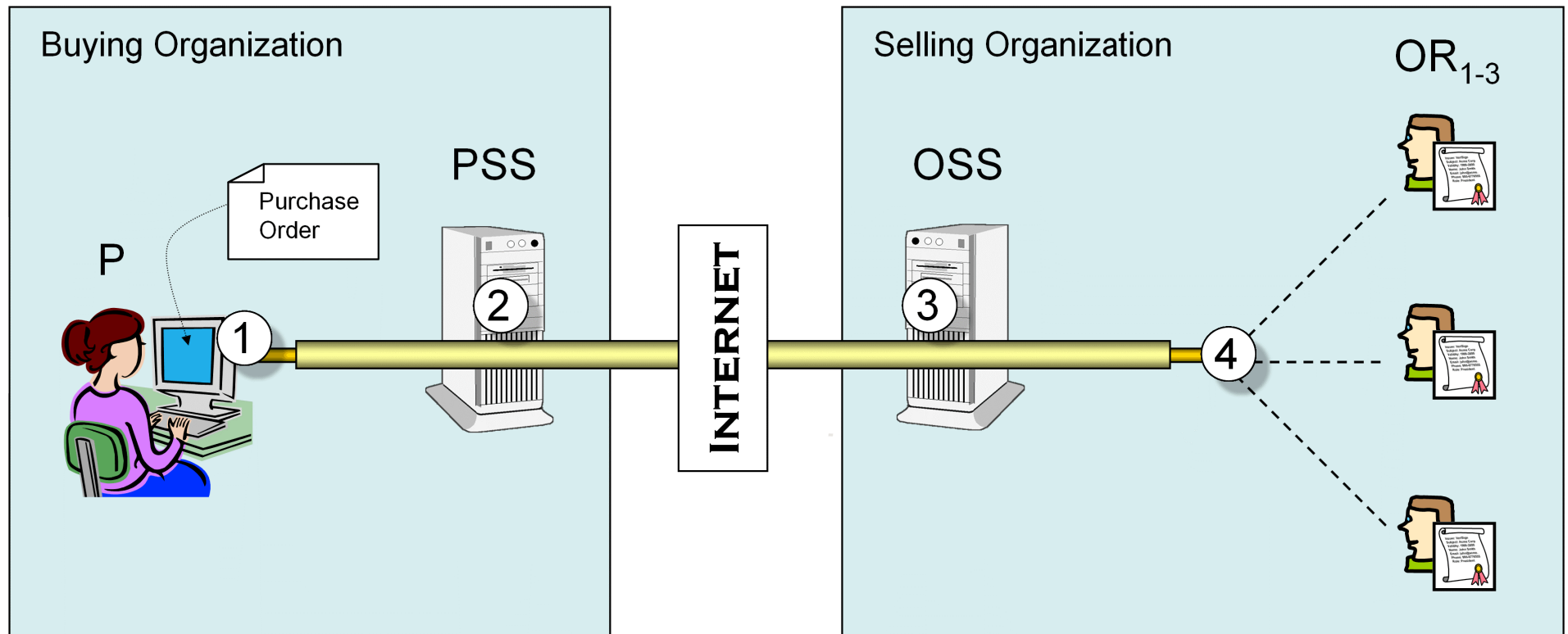
This particular document shows how the classic enterprise PKI model [1] like the US Federal PKI is *presumed* to be applied to e-purchasing. That I write “presumed” is because to date hardly anything has been published [2] regarding the combination of PKI and common business processes. One of the core components of an enterprise PKI is publishing employee certificates in directories, mainly to enable a very vital aspect of security, namely confidentiality. However, as seen on the next page, this is not as straightforward as it may sound, here only touching a fraction of the issues actually involved in publishing and retrieving employee related information.

### Notes:

1] An enterprise PKI using the author’s definition is a PKI where each employee or associate is equipped with a digital certificate not only identifying the individual, but the employer as well. Due to the latter, such certificates are usually intended to be usable both within the enterprise as well as in external enterprise-related communication.

2] The financial industry has indeed documented a number of PKI-using payment protocols like SET and 3D Secure but payments have a much more limited scope than identity-based schemes.

# End-2-end encryption when applied to common business processes raises many interesting questions



1. How is the purchaser (P) going to select and acquire a suitable Order Receiver (OR) encryption certificate from the selling organization?
2. How is the buying organization's Purchasing System Server (PSS) able to perform its logging, authorization, and control tasks if purchase orders already have been encrypted by the Purchaser using a public key from an external selling organization?
3. How is the selling organization's Order System Server (OSS) supposed to decipher and validate incoming orders if they are encrypted by a public key of a specific Order Receiver (OR<sub>n</sub>) employee? In case the designated OR is unavailable, how is OSS going to be able to delegate order handling to another OR?
4. How are different Order Receivers (ORs) supposed to cooperate if they cannot see each others' tasks? Are the particular Order Receiver and Purchaser also the natural entities for handling associated invoices?

Clear text data  
Encrypted data

Regarding reasonable answers to these questions, the following seems to be the reality: *The concept of a centralized, collaboration oriented information system appears to be largely incompatible with the client-centric nature of the enterprise PKI model.*

However, the vast majority of enterprise information systems indeed build on information consolidation and accumulation. Many enterprises such as airlines and banks depend almost entirely on such systems.

To augment an enterprise PKI with other means to achieve message encryption is indeed quite possible but this also imposes questions regarding the viability of the scheme as a whole, *and in particular its reliance on more or less public directories.*

It is in this context important to note that for *internal operations*, directories already have a major utility in most large organizations, regardless if they use PKI or not.

### **The succeeding lessons**

In the next lesson we will study how a different PKI architecture can reduce the problems associated with message encryption. This architecture is derived from “pre-PKI” business-oriented security solutions like leased lines. In a subsequent lesson we will also apply digital signatures to e-purchasing, something which is actually even more complex than encryption.

### **About the author**

The author is a senior system software architect and developer, working with software ranging from low-level APIs to information systems. PKI is a special interest of mine since 1996, when I begun looking into the now defunct Swedish ID-card program. The author may be reached at [anders.rundgren@telia.com](mailto:anders.rundgren@telia.com)

### **Disclaimer**

This work is not to be associated with my employer, it is an entirely private mission and the views expressed are mine.