Practical considerations using eSeals

Albert Krohn, Michael Beigl, Christian Decker, Philip Robinson and Tobias Zimmer
Telecooperation Office, Universität Karlsruhe
Vincenz Priessnitz Str. 1, 76131 Karlsruhe
{krohn, michael, cdecker, philip, zimmer}@teco.edu

ABSTRACT
While in the past waxed-seals where used to ensure the integrity, electronic devices are now able to take over this functionality and provide better, finer grained, more automated and more secure supervision. This demo shows a prototype eSeal system, with a computational device at its core that can be attached to a good and can be configured automatically using active tags. The eSeal monitors and seals different states sensed from the object's physical conditions. The eSeal is designed and implemented with flexibility in mind, allowing configurable integrity control settings. The system works with minimal infrastructure requirements and is functionally self-contained, such that goods can be supervised that are only accessible in certain locations. A major output of the eSeal prototype system demo is the support for intuitive user interaction, with regards to configuration and handling of the devices in the activity chain.

Keywords
Product monitoring, eSeal, security system, user interface

INTRODUCTION
International trade sees the shipment of goods across borders in different containers and stored in different locations and conditions. There are therefore threats to economic and safety due to the risk of sabotage, smuggling and degradation of goods [3]. There is therefore a mandate on all "control points" in a supply chain to contribute to security and/ or quality checks on goods in storage or transit. In former times objects of value like documents, deeds, contracts, goods for trade, and other articles, were stored in a container, which in turn was sealed with wax and the imprint of a seal ring (bearing an insignia) or a plumb. The object's authenticity was detectable through the seal ring imprint on the wax and the integrity could be discerned by inspecting for either of the two physical states of the seal - *intact* or *broken*. However, as demonstrated in this prototype system, modern sensor and communication technology provides advanced methods for protection of objects of value.

The eSeal prototype (see Fig. 1) presented in this demo can be applied to physical goods to claim and assert states but doesn't protect the object itself. It is therefore an augmented *indicative* seal rather than a *barrier* seal. It can however collect context information about sensed violations and can actively and autonomously monitor and issue alerts. The eSeal can exchange relevant information with other computer systems, maintaining a fine-grained correlation of physical conditions and an interpretation in the information world.

Fig. 1. eSealed good (hard disc) in transit.

eSeal DEMO SYSTEM
We demonstrate an eSeal prototype system with different physical components to perform the typical eSeal security tasks. With this demo, we want to show how support for implicit interaction can lead to more intuitive configuration and handling of the eSeal system. The hardware modules on display are based on the particle computer wireless platform[1]. We are therefore able to "seal" various "integrity properties" with the prototype system. These integrity properties are explained by example:

1. *Conditional Integrity*. Given internal properties (temperature, pressure…) must be maintained.
2. *Relational Integrity*. Given obligation or refrain properties in relation to other goods, such as proximity, must be maintained.
3. *Authorization Integrity*. Interactions and transactions must be limited to authorized parties and roles.
4. *Environmental Integrity*. Given external properties (location, temperature, pressure…) must be asserted.

eSeal CONFIGURATION
Before an eSeal can be applied we need to configure what are the integrity conditions for a certain good. This is done by an active tag on the good itself. The active tag contains

a number of rules describing exactly these conditions, but it cannot check them against violations. Rules may contain directives like the temperature must not exceed 30 degree Celsius or the good must not exposed to light longer than 30 minutes.

eSeal ACTIVITY CHAIN

The eSeal activity chain, presented in Figure 2, shows the most important system elements and tasks: *initialization*, intermediate *checkpoints,* and *removal* at the receiver.

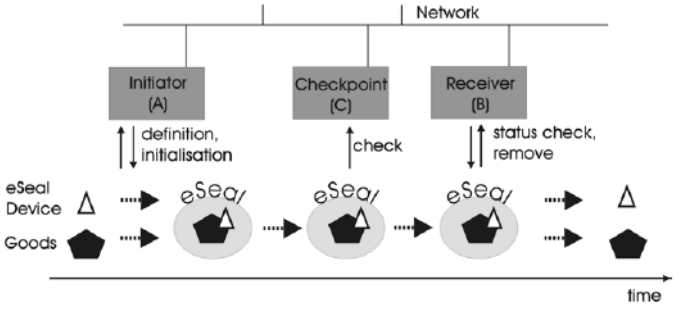

Fig. 2. eSeal Activity Chain

The steps of this activity chain are part of the eSeal demo and are now explained:

1. The Initiator combines the eSeal device and the goods and initializes the eSeal device in order to seal the goods.
   In the demo prototype system, the integrity conditions are informed by the good itself through an active tag. The eSeal device is able to receive these conditions. Equipped with various sensors it can perform different types of integrity assertions. The initialization is done with a special authorized initialization device. When the active tag, the eSeal device and the authorization device are together in close range, the eSeal will be applied to the according good and the eSeal device will start the necessary tasks such as sensor readings and communication.
2. At a checkpoint, the status of the eSeal (valid or broken) can be observed.
   In the demo prototype system the checkpoint is a mobile display that shows the user the state of the eSeal (valid or broken) and further information on the eSeal device, good etc.
3. The receiver removes the applied eSeal device from the physical good to finish the activity flow of the eSeal system.
   In the demo prototype system, this removal is done by an authorized receiver device that has to be in range of the eSeal. It deactivates the eSeal, which can then be physically removed

During the transition of the "esealed" good the according integrity will be guaranteed by the eSeal. The demo system shows a hands-on experience of the eSeal. If an eSeal is applied on a good, a user can take the good and play with it and test the eSeal. If e.g. the eSeal is removed from the good, it will change its state to "broken". If an integrity is violated like too strong acceleration, the eSeal state will as well change to "broken". The checkpoint device can be used at any time to visualize and audit the actual state of the eSeal.

eSeal DEMO EXAMPLE

This eSeal demo example should clarify the focus and actual content of the demo. An example might be the transport of perishable goods like fresh vegetables. For the transport of those goods there are three major points to be assured: The goods must not be exposed to sunlight for an extended time, hence must be cooled, and may have a limited transport duration. To understand this in the integrity classes, the two integrities *conditional* and *environmental integrities* are involved. The eSeal device can in this case assure the allowed temperature through a sensor as well as the light exposure and will carry a real time clock to observe the time elapsed since the initialization of the seal. In the demo setting different hardware parts will be involved: *the good* (represented by a plastic copy) will carry an active tag, defining the integrities to be realized in the eSeal. The *eSeal device* itself carrying the sensors and communication, a *checkpoint device*, the *authorization device* and the *reception device*. The user takes the good, applies an eSeal device by simply attaching it physically to the object and then brings the authorization device in range to initialize the eSeal. It then becomes active. At any time, the user can bring the checkpoint device to the goods and review the state of the eSeal. While the good is in transit the user can intentionally break the seal by exposing the good content to e.g. environmental light or by exceeding the transit time of the eSeal (and the good) between authorization device and reception device. At the end of the virtual transport, the user will take the reception device and bring it close the goods with the eSeal device and through this will deactivate and remove the eSeal in an authorized way.

REFERENCES

1. The particle computer website: *http://particle.teco.edu.* accessed 05/2004.
2. Decker, C., Beigl, M, Krohn, A., Kubach, U., Robinson, P. "eSeal - A System for Enhanced Electronic Assertion of Authenticity and Integrity of Sealed Items". Pervasive 2004, Wien, Austria, LNCS, Vol. 3001, pp.254-268.
3. Wolfe, M. "Electronic Cargo Seals: Context, Technologies and Marketplace", July 12, 2002. Prepared for: Intelligent Transportation Systems Joint Program Office Federal Highway Administration U.S. Department of Transportation