Tokeneer Requirements Specification

Supplement to Requirements Presentation

What is Tokeneer?

- Software system for controlling access to a high-security area
- Developed so that security and other requirements could be formally verified
- Requirements specification is contained on a large document
  - Approach is mainly through Use Cases
Tokeneer Requirements Specification

• Functional (behavioral) requirements through eleven (11) Use Cases
  – Each use case covers a key scenario
• Some supplementary diagrams as well
  – Some for non-functional requirements

5 Behavioural Requirements

The required behaviour of the ID Station is specified here using scenarios, which run through typical uses of the ID Station and define the interaction between the ID Station and its connected systems. In each case the scenario focuses on a successful outcome, but it also covers various conditions that may arise that do not allow the successful outcome to be achieved. The full behaviour of the system, including both successful and failed outcomes, constitute the system requirements.

The scenarios considered are:

1. User gains allowed initial access to Enclave
2. User is denied prohibited initial access to Enclave
3. User gains allowed repeat access to Enclave
4. ID Station is started and enrolled with input from the Enrolment Station
5. ID Station is started already enrolled
6. ID Station is shut down
7. Security Officer updates the configuration of the ID Station
8. Audit log is archived
9. Guard manually unlocks the door
10. Administrator logs on
11. Administrator logs off
5.2 Scenarios

5.2.1 User gains allowed initial access to Enclave

Description
A User who should be allowed access to the enclave is given access, making use of biometric authentication.

Stimulus
User inserts a smartcard into the smartcard reader.

Assumptions
ScGainInitial.Ass.ValidStart
The ID Station has valid start-up data.
ScGainInitial.Ass.ValidConfig
The ID Station has a valid data configuration.

Introduction

Some of these are environmental requirements

Here is a timing Requirement. Should it be Said better?

Functional Requirements (when combined with assumptions)
Robustness requirements

Anticipating Requirements Validation and Design
5.2.10 Administrator log on

Description
An Administrator logs onto the ID Station by inserting their Token in the Admin Token Reader.

Stimuli
A Token is inserted in the Admin Token Reader.

Assumptions
SucLogOnADMIN.
The ID Station is quiescent (no other access attempts, configuration changes or start-up activities are in progress).

SucLogOn-Door-Secured.
The door is closed and locked.

SucLogOn-Admin-ValidAdmin.
The card inserted by the Administrator has a valid Authorization Certificate.

Success End-conditions
SucLogOn-SuLogOn
The ID Station is available for use by the Administrator, in that it will respond to the commands allowed by that Administrator as defined by the privileges in the Authorization Certificate read from the Token and the Configuration data held on the ID Station.

SucLogOn-SuLogOn-Door-Secured.
The door is closed and locked.

SucLogOn-SuLogOn-Audit.
The following events have been recorded in the Audit Log (in any order), and the existing audit records are preserved:
- Log-on by Administrator
- Insertion of card
- Reading data from card (possibly multiple failures, but at least one success)

Failure Conditions
SucLogOn-Fail-ReadCert.
The card inserted by the Administrator does not allow all its necessary data to be successfully read, possibly due to being incorrectly inserted in the first place, being a faulty card, having the incorrect information on it, or being removed before all the information has been read. The set of data to be read is:
- Authorization Certificate

SucLogOn-Fail-Audit.
Audit file cannot be successfully written. Result: the Door is locked and the system is shutdown.

SucLogOn-Fail-Audit-Preserve.
Space for audit files has been exhausted. Result: the oldest audit records are overwritten with the new audit records, and an alarm is raised by the Guard.

Constraints
SucLogOn-Door-Secured.
No ID Station shutdown or User use will be allowed during this scenario.

Rationale
SucLogOn-Admin-ValidAdmin.
Only the Authorization Certificate is checked, because we assume that the purpose of the Authorization Certificate is to control access to the workstations within the station, and for these purposes the ID Station acts as a workstation. The ID, IIA and Privilege Certificates will have been used to gain entry to the environment.

5.2.11 Administrator log off

Description
An Administrator logs off the ID Station.

Stimuli
The Token is removed from the Admin Token Reader.

Assumptions


There is still a need to coordinate and integrate what these scenarios say
Use of Diagrams to Augment the Use Cases

- Not all of our requirements types were addressed by these use cases
- Some of them are addressed separately from the use cases
- Some diagrams are redundant with use cases (to support cross checking)
- Some diagrams could/should be embedded in some of the use cases
There are two system boundaries of interest in the development of this variant: the boundary between
the ID Station machine and its environment (including its peripherals); and the boundary between the ID
Station core functions and its support functions. These boundaries are expanded below.

Environmental requirements

4 System Context
The section defines the system boundary for the high integrity variant of the ID Station, and explains
which elements will be developed by whom, and by what process.

The existing ID Station model given in section 3, we can re-present it showing how the elements
will be re-developed.
Artifacts are needed in order to specify functional/behavioral requirements

3.2 Biometrics

All of the complexity of the biometrics is hidden within the biometric library, which we will be simulating in a very simple way, enabling the test drivers to decide whether a fingerprint will or will not match a template.

3.3 Door/Latch

The door has four possible states: the cross product of open/closed and locked/unlocked.

Open means the door does not prevent a human from entering or leaving the enclave.

Closed means the door prevents a human from entering or leaving the enclave. To enter or leave, the door must first be opened.
Augments Functional Rqmt.
Security Requirement?

As unlocked states are potentially insecure, there is always a time-out period, after which the door will be commanded to lock.
Figure 7.2: Administrator logon/logoff state transitions

The context for administrator login is given below.

6 Design Constraints

The system will be developed and run on a workstation running NT 4.0.