Tickets, Entrittskarten zu Anwendungen der Campuskarte

Thomas J. Wilke

Vortag am PRZ der TU Berlin

Berlin, den 20.07.2001

Gliederung

- Was ist ein Ticket?
- Wie werden Tickets bei der Campuskarte eingesetzt?
- Warum wird ein ticketbasiertes Verfahren eingesetzt?
- Single Sign On, wofür?

Was ist ein Ticket?

Definitionen

- **Abstrakte Definition**

  Ein Ticket ist ein Objekt dessen, Authentizität nachweisbar ist und das die Identität eines Subjektes in einer definierten Umgebungen sowie für einen definierten Zeitraum abstrakt beschreibt.

- **Anschauliche Definition**

  Ein Ticket ist eine „Eintrittskarte“ für Nutzer zu Anwendungen, die die Campuskarteninfarstruktur nutzen. d. h. derjenige Nutzer der für die von ihm angeforderte Anwendung eine gültige „Eintrittskarte“ besitzt, erhält Zugang zu der Anwendung.

Was ist ein Ticket?

technische Einordnung

Protokollebene	Identifikation einer / eines	Mechanismus	Lebensdauer	Inhalt
ICMP	Netzwerk-schnittstelle	MAC	Geräteeinsatz	Geräte-nummer
IP	Netzknotens (z.B.Rechner)	IP-Adresse	Netzwerk-einsatz	4 Zahlen
TCP/UDP	Prozess eines Rechners	Port-Nr.	eines Prozesses	Zahl
SSL	gesicherte Verbindung	Masterkey	Verbindungs-dauer	lange Zahl
SSO / SC	Benutzer	Ticket	Nutzung des Browsers	OM, PS, Gültigkeit

Was ist ein Ticket?

Struktur der verwendeten Tickets

User Ticket

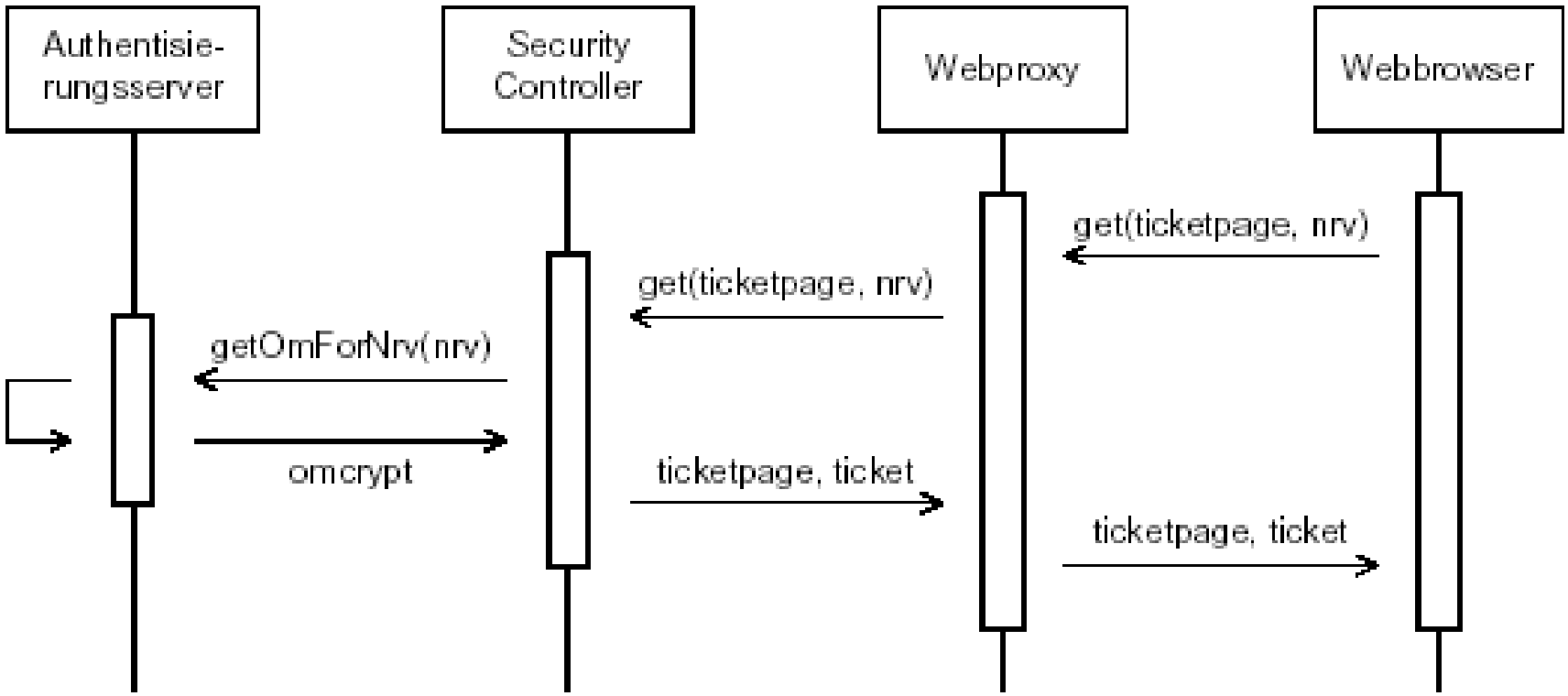
- Ausstellungszeit
- Gültig bis
- IP-Nummer
- SSL-Key
- Data:
  - OM (Ordnungsmerkmal)
  - PS (Personenstatus)
  - von
  - bis
  - applikationsspezifische Daten

Domain Ticket

- Host1
- Host2
- Host3

Ticketeinsatz bei der Campuskarte:

Verwendung der Tickets



Ticketeinsatz bei der Campuskarte:

Außerkraftsetzung von Tickets

Durch das System

- Begrenzung der Gültigkeitsdauer eines Tickets

Durch den Anwender

- Beenden des Browsers
- Entfernung der Karte aus dem Kartenleser

Durch eine TU-Instanz

- Sofortige Sperrung pro Anwendung
- Globale Sperrung in Echtzeit
  (verlängerbares Ticket: Bedienugskomfort <-> Sicherheit)
- Später: globale oder dezidierte Sperrung mit sofortiger Wirkung (Einsatz eines rollenbasierten Zugriffkontrollsystems)

Warum wird ein tickerbasiertes Verfahren eingesetzt?

- Das Verfahren hat sich bei anderen Systemarchitekturen bewährt (z. B. Kerberos)
- Rein HTTP-basiertes Verfahren
- Ermöglicht hohe Einsatzflexibilität
- Ermöglicht einen hohen Bedienungskomfort für die Anwender
- Bietet höheres Maß an Sicherheit als die bisher etablierten Verfahren

Single Sign On?

Zielsetzung

Mit einem Authentisierungsvorgang mehrere Anwendungen nutzen zu können soll:

- den Bedienungskomfort erhöhen:
  Verminderung der PIN-Eingaben, schnellerer Zugang zur Applikation
- die Authentisierungsinfrastruktur entlasten
- die Sicherheit erhöhen:
  höhere Akzeptanz der Sicherungsverfahren bei den Anwendern, Abwehr von DoS-Attacken durch Nutzung vorhandener Kontrollinstanzen