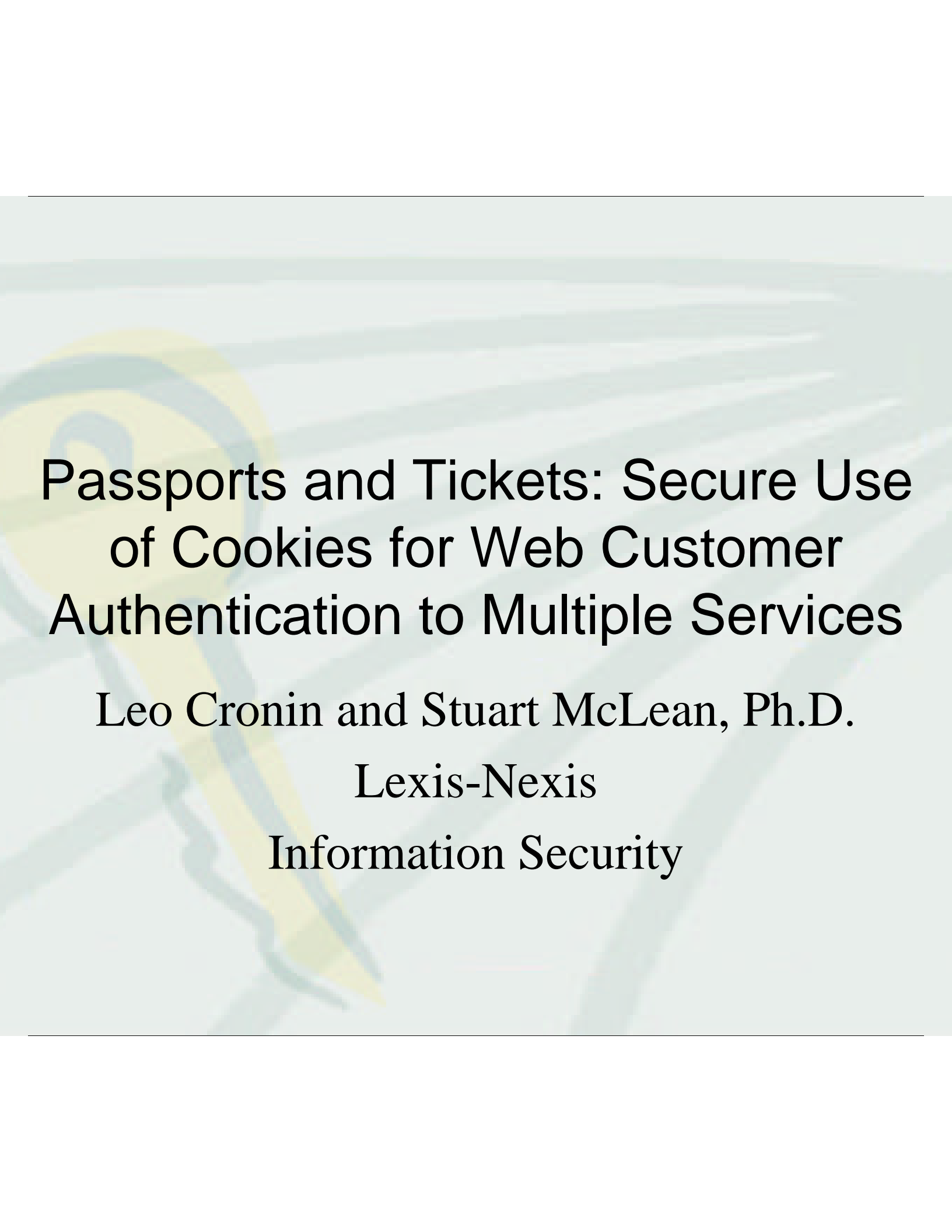


---



# Passports and Tickets: Secure Use of Cookies for Web Customer Authentication to Multiple Services

Leo Cronin and Stuart McLean, Ph.D.

Lexis-Nexis

Information Security

---

---

# LEXIS-NEXIS and the Internet

Over 2 billion documents in ~8700 data bases

1.6 million users (growing)

Commercial use of Internet since early '90's

- Education market
- Telnet interface to “classic”, session manager based system
- Major Law Firms and Corporations since late '96
- Web products emerge in '97

Integrity, confidentiality and availability = LEXIS-NEXIS

Internet poses major confidentiality challenges

---

---

# Issues/Assumptions with Web Products

Customers want hands-off authentication

Customers do not want delays caused by SSL

Authentication protects LEXIS-NEXIS, not the customer

Authentication infrastructure using standard mechanisms

Authentication must apply to multiple services/products

---

---

# What are cookies?

Tokens accepted and managed by browsers for maintaining state

Cookie distribution can be permitted throughout the domain that delivered them

Persistent cookies are the same tokens which may be directed to a browser-controlled client file

Server only controls:

- Persistence (most browsers warn)
  - Content of cookies
  - Availability of cookies to other hosts
-

---

# Proposal

Use long-lived cookies (Passports) for authentication

Use short-lived time-stamped cookies (Tickets) for session maintenance

Re-authenticate in background at fixed intervals

Re-authentication intervals may vary with products

Passports may be saved for very long-term transparent authentication (months)

---

---

# Proposal (continued)

*Use SSL for all transmission of Passports*

Utilize a single, separate authentication server for generating Tickets

Products worry only about Tickets

Policies built into the Authentication server

Passports can be cancelled with password change or revocation of account in the central authentication database

---

---

# Proposal (continued)

Authentication server is compatible with

- Forms based authentication
- BASIC authentication
- Certificate based authentication
- IP authentication
- Customer entitlements
- Biometric APIs?

Authentication issued this way would be product independent

---

---

# Advantages

Reusable cookies (Passports) would always be protected under SSL

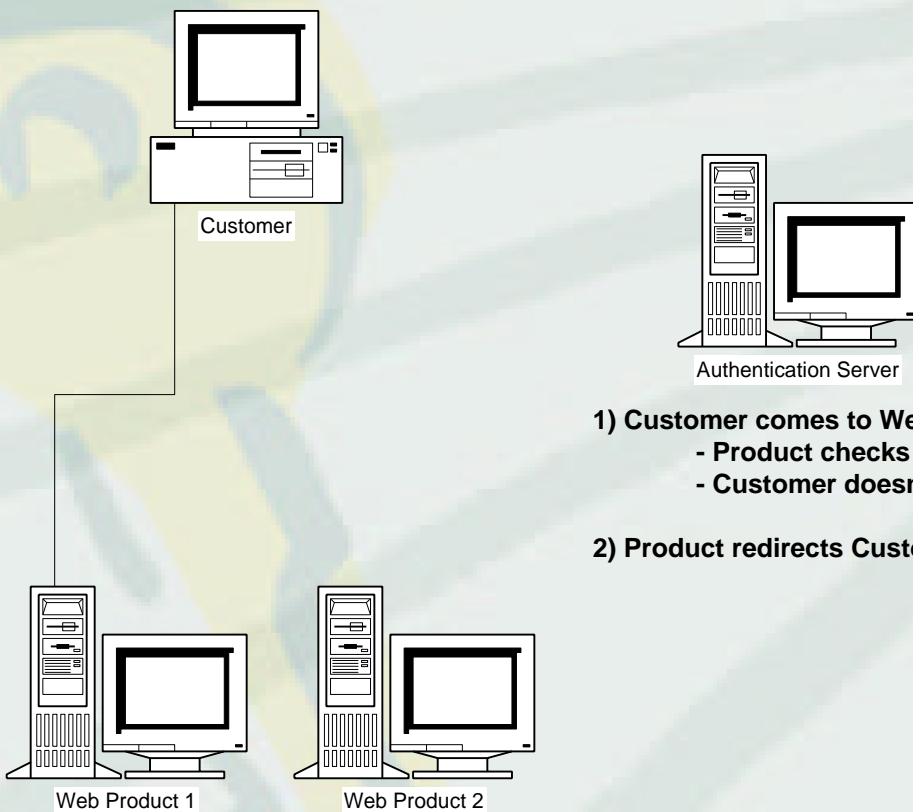
Display pages would not have to use SSL to assure login integrity (Customer confidentiality would still require SSL on some pages)

Control over Authentication would be centralized and standardized across products

Trips to customer databases would be reduced

---

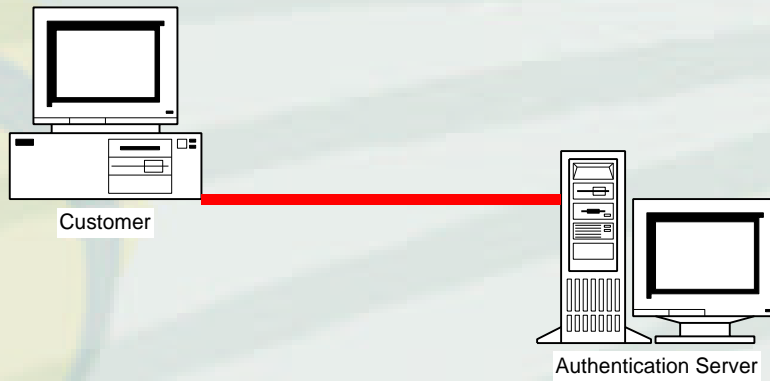
# Protocol Walkthrough



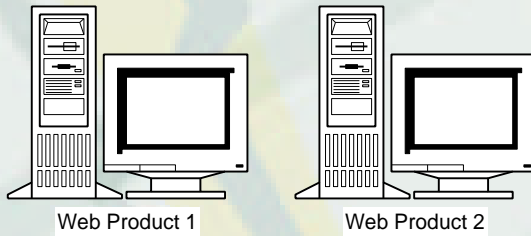
- 1) **Customer comes to Web Product 1**
  - Product checks for Ticket
  - Customer doesn't have one

- 2) **Product redirects Customer to Authentication Server**

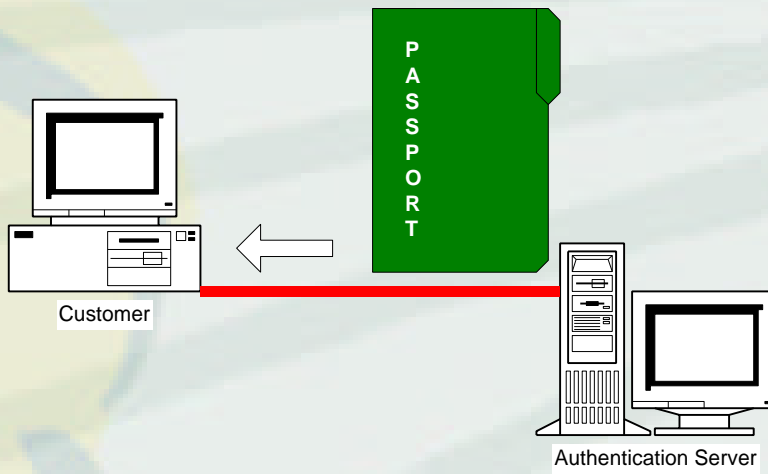
# Protocol Walkthrough



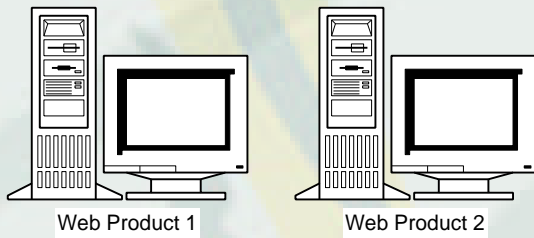
- 3) **Authentication Server checks for Passport**  
- Customer doesn't have one
- 4) **Authentication Server requires login**  
- Customer logs in successfully



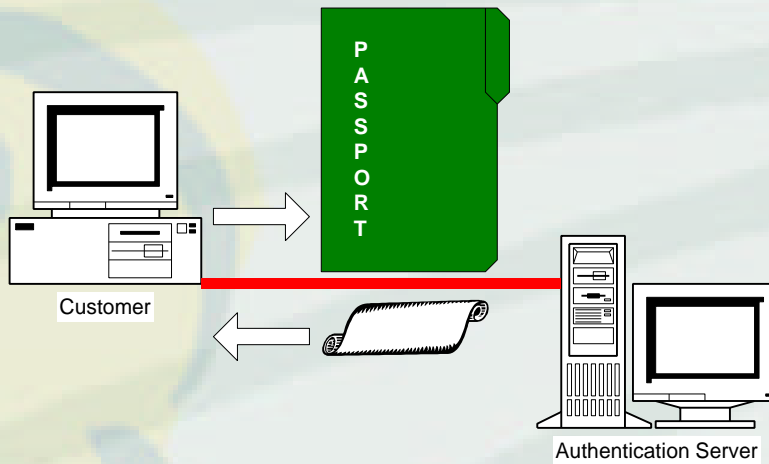
# Protocol Walkthrough



**5) Authentication Server issues Passport**



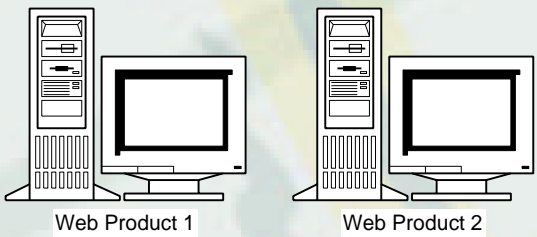
# Protocol Walkthrough



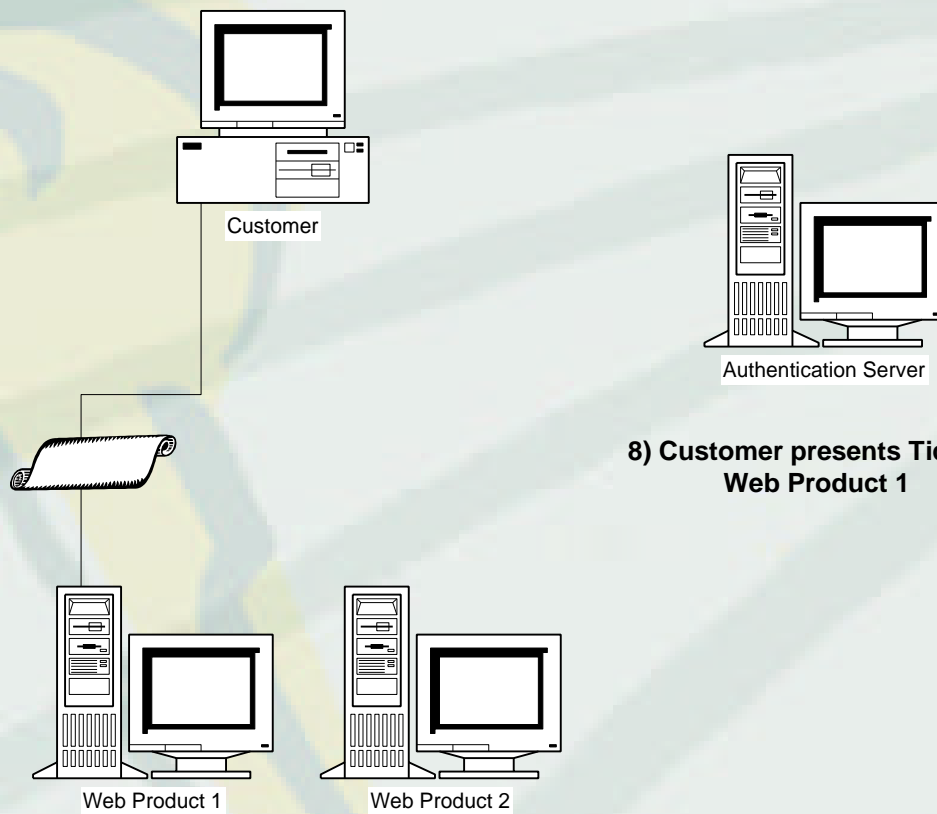
## 6) Customer presents Passport

- Authentication Server validates against Revocation List
- Authentication Server checks Entitlements against ICUST

## 7) Authentication Server issues Ticket

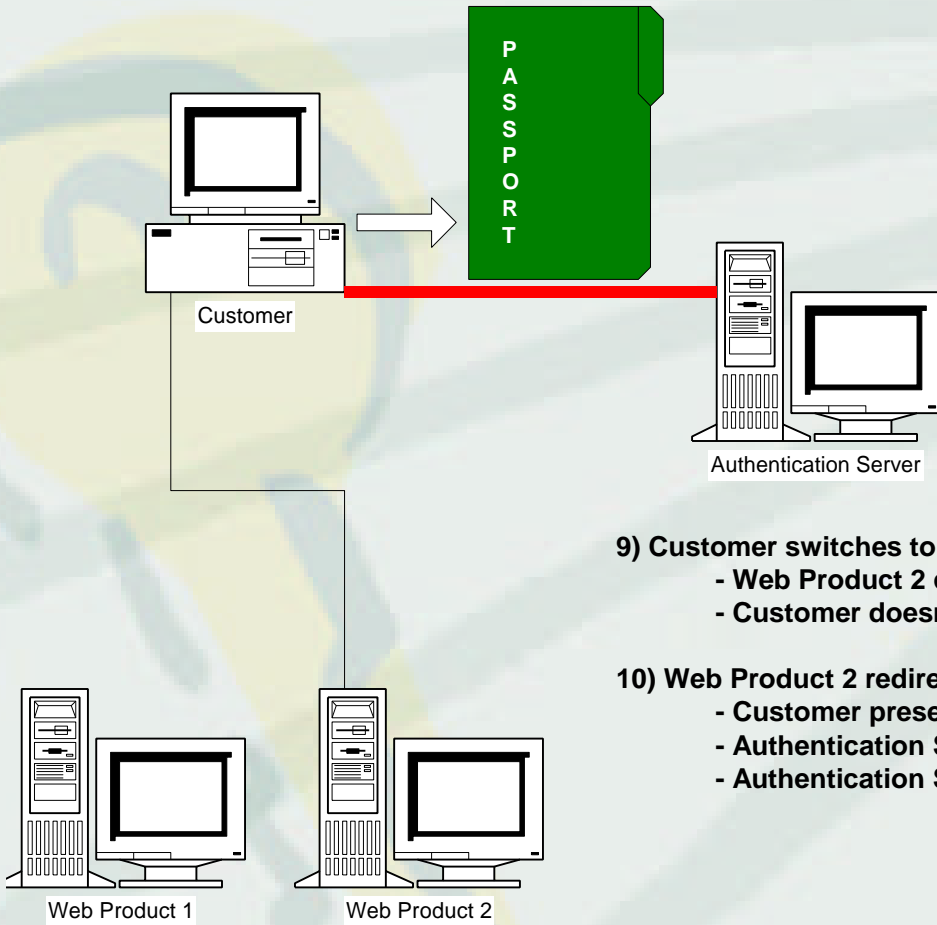


# Protocol Walkthrough



**8) Customer presents Ticket - granted access to Web Product 1**

# Protocol Walkthrough



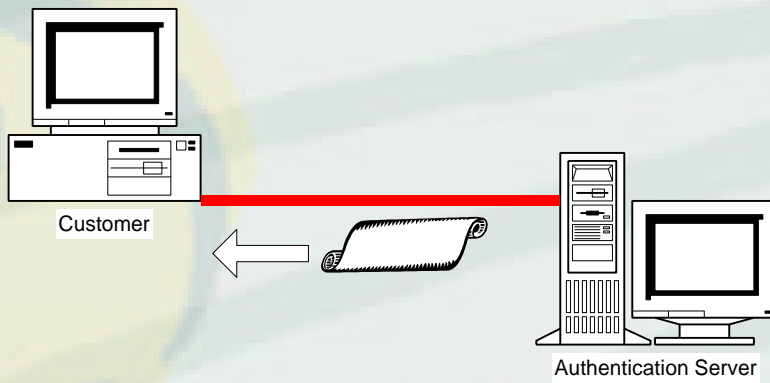
## 9) Customer switches to Web Product 2

- Web Product 2 checks for Ticket
- Customer doesn't have one for Web Product 2

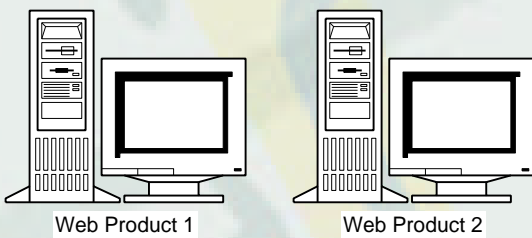
## 10) Web Product 2 redirects to the Authentication Server

- Customer presents Passport
- Authentication Server validates against Revocation List
- Authentication Server checks Entitlements against ICUST

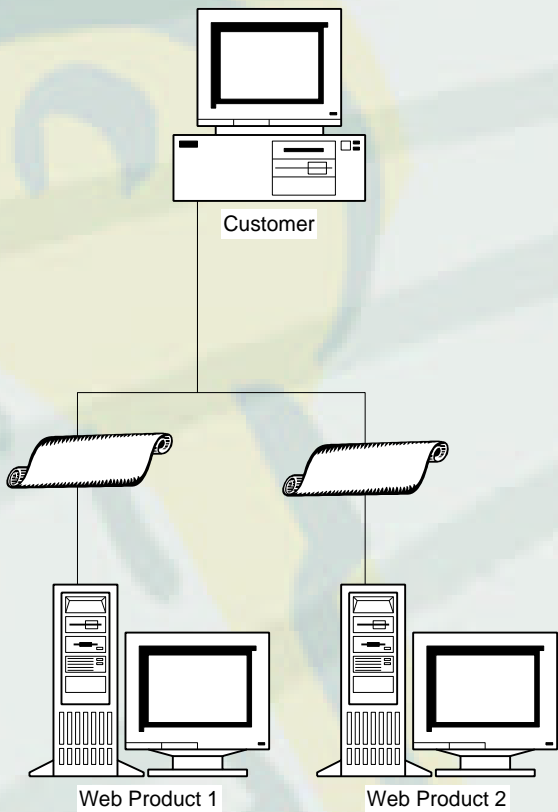
# Protocol Walkthrough



**11) Authentication Server issues Ticket for Web Product 2**

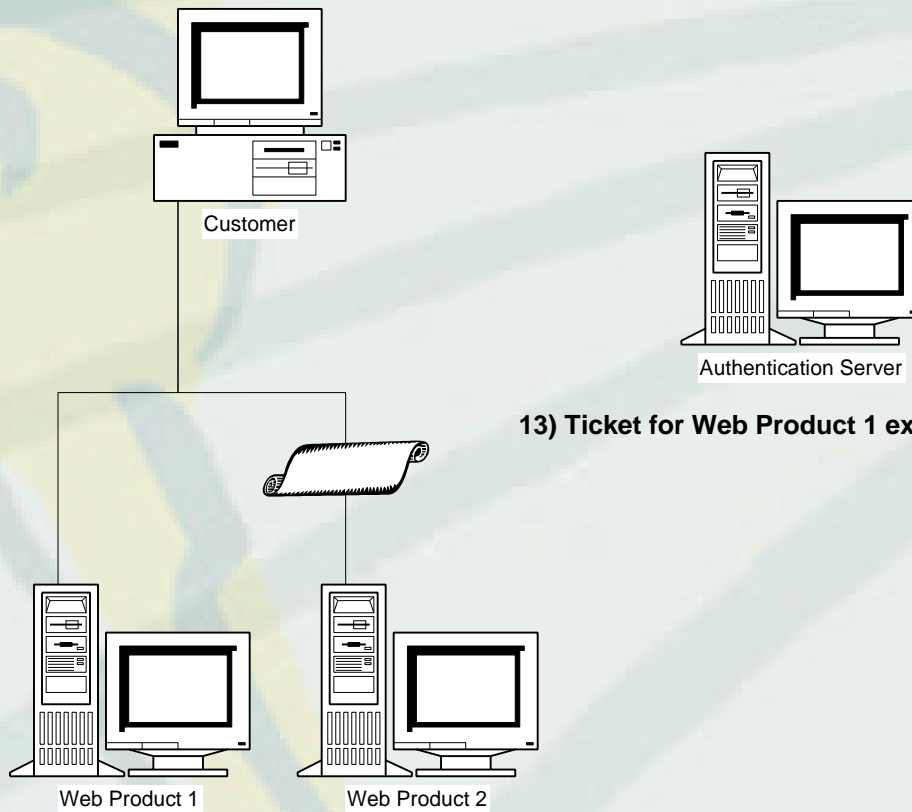


# Protocol Walkthrough



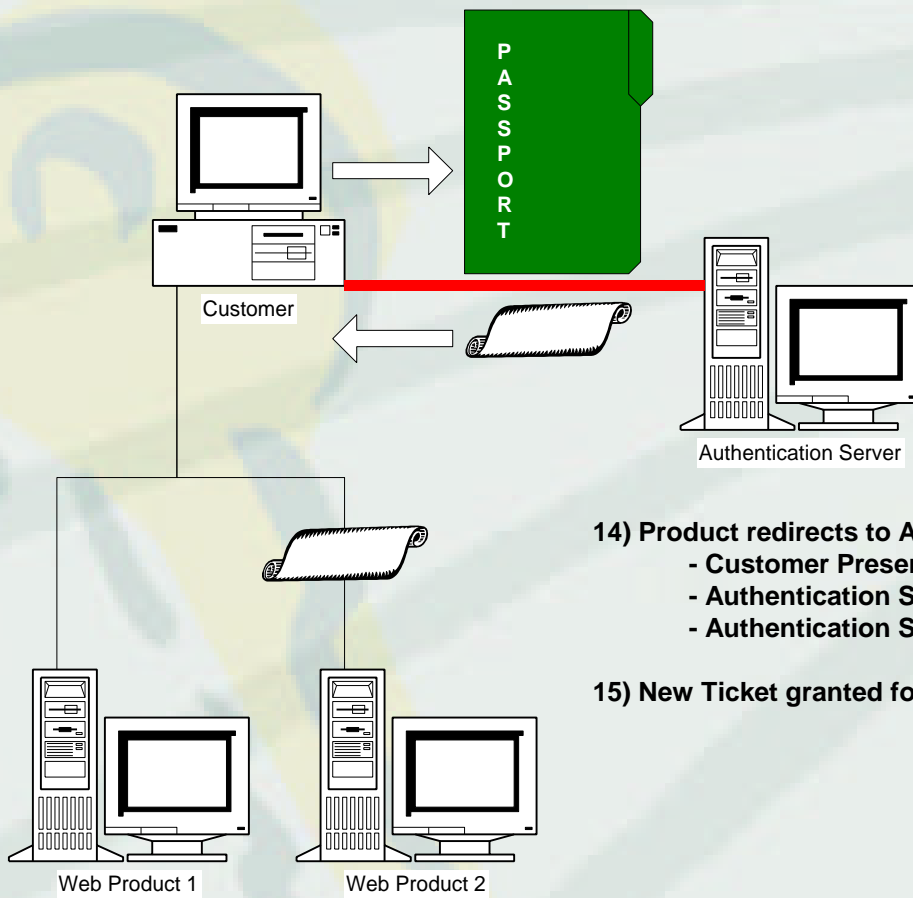
**12) Customer has live connections with both Web products**

# Protocol Walkthrough



**13) Ticket for Web Product 1 expires after 15 minutes**

# Protocol Walkthrough

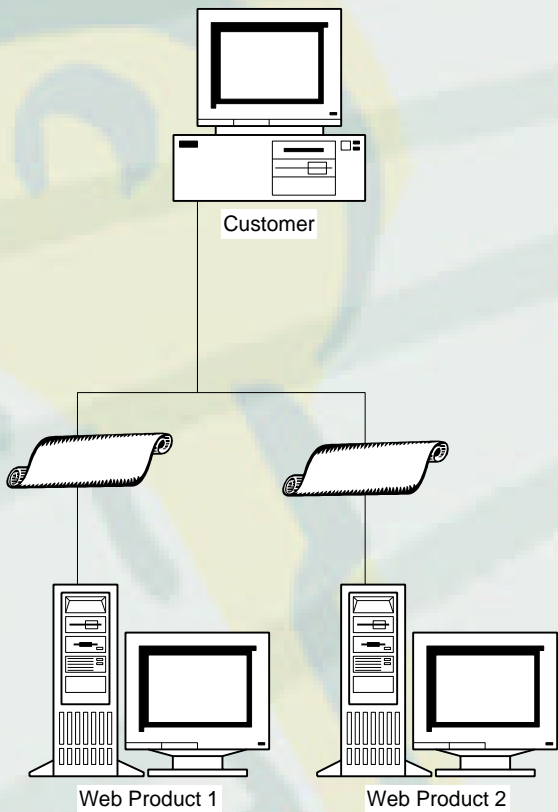


## 14) Product redirects to Authentication Server

- Customer Presents Passport
- Authentication Server validates against Revocation List
- Authentication Server checks Entitlements against ICUST

## 15) New Ticket granted for Web Product 1

# Protocol Walkthrough



**16) Customer has live connections with both Web products**