Supported by
the Belgian
Walloon Region

Authenticated Wireless Roaming via Tunnels

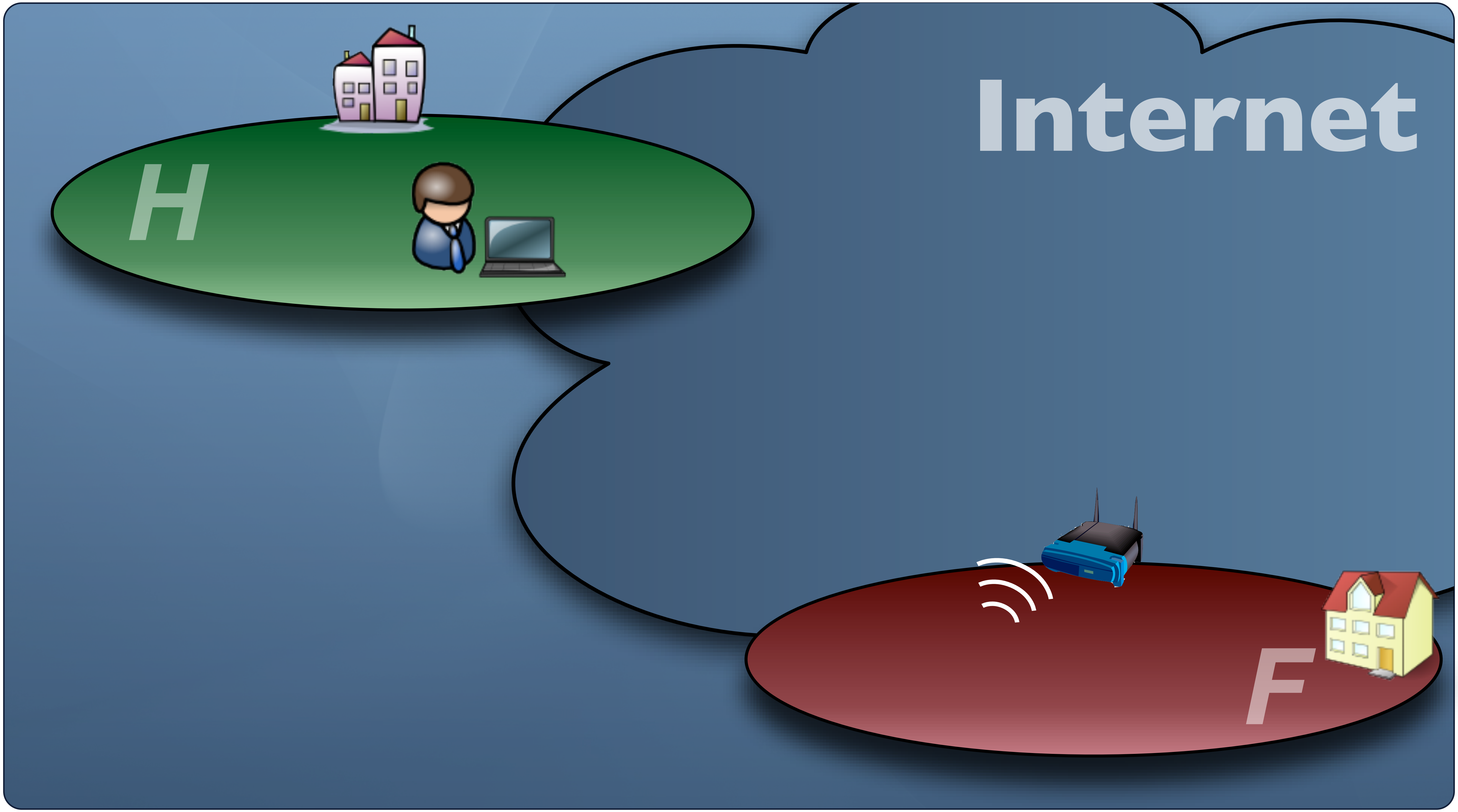
Making Mobile Guests Feel at Home

M. Manulis, D. Leroy, F. Koeune,
O. Bonaventure, J-J. Quisquater

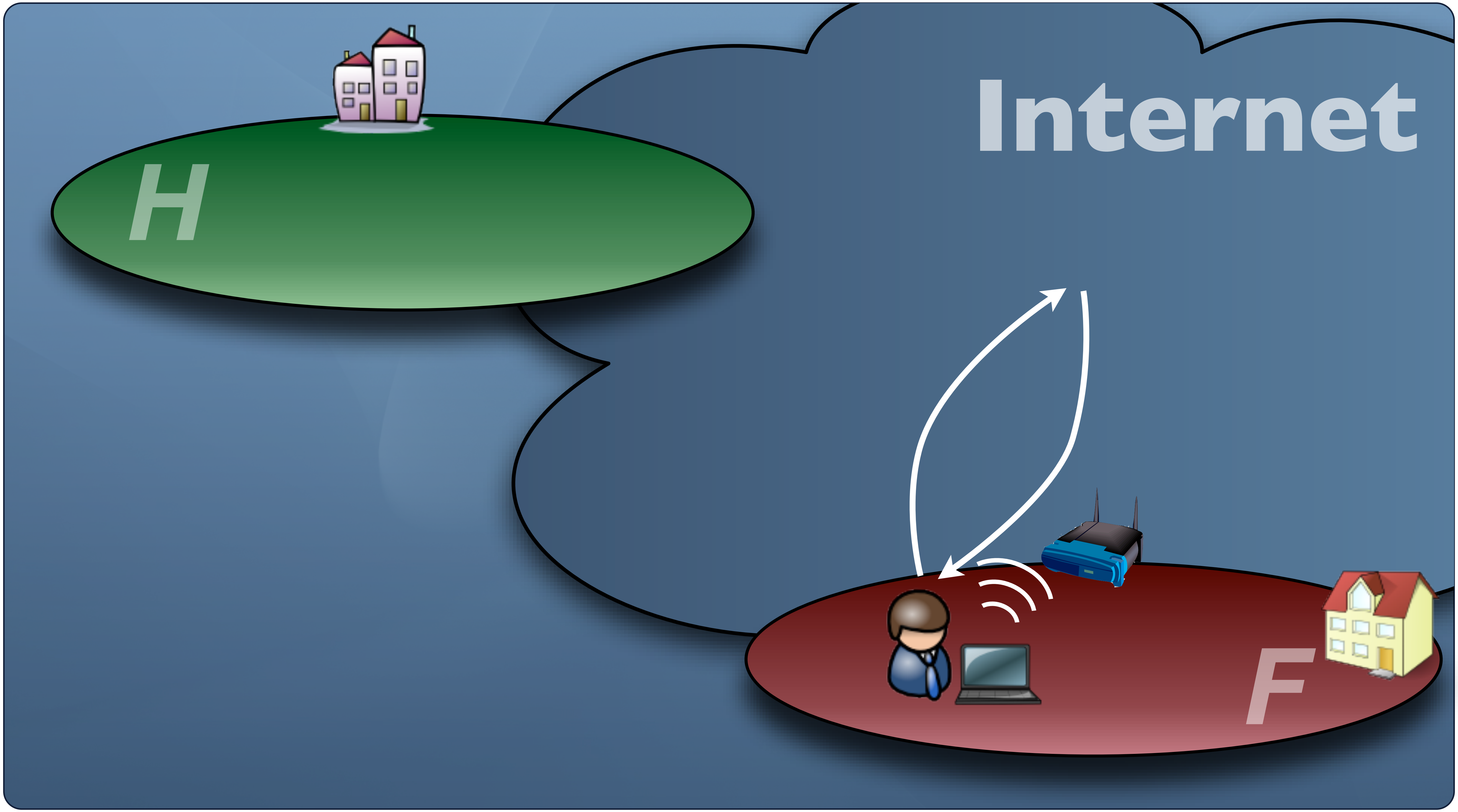
UCLouvain - Belgium
UCL Crypto Group - IP Networking Lab

ASIACCS'09 - March 10-12, 2009

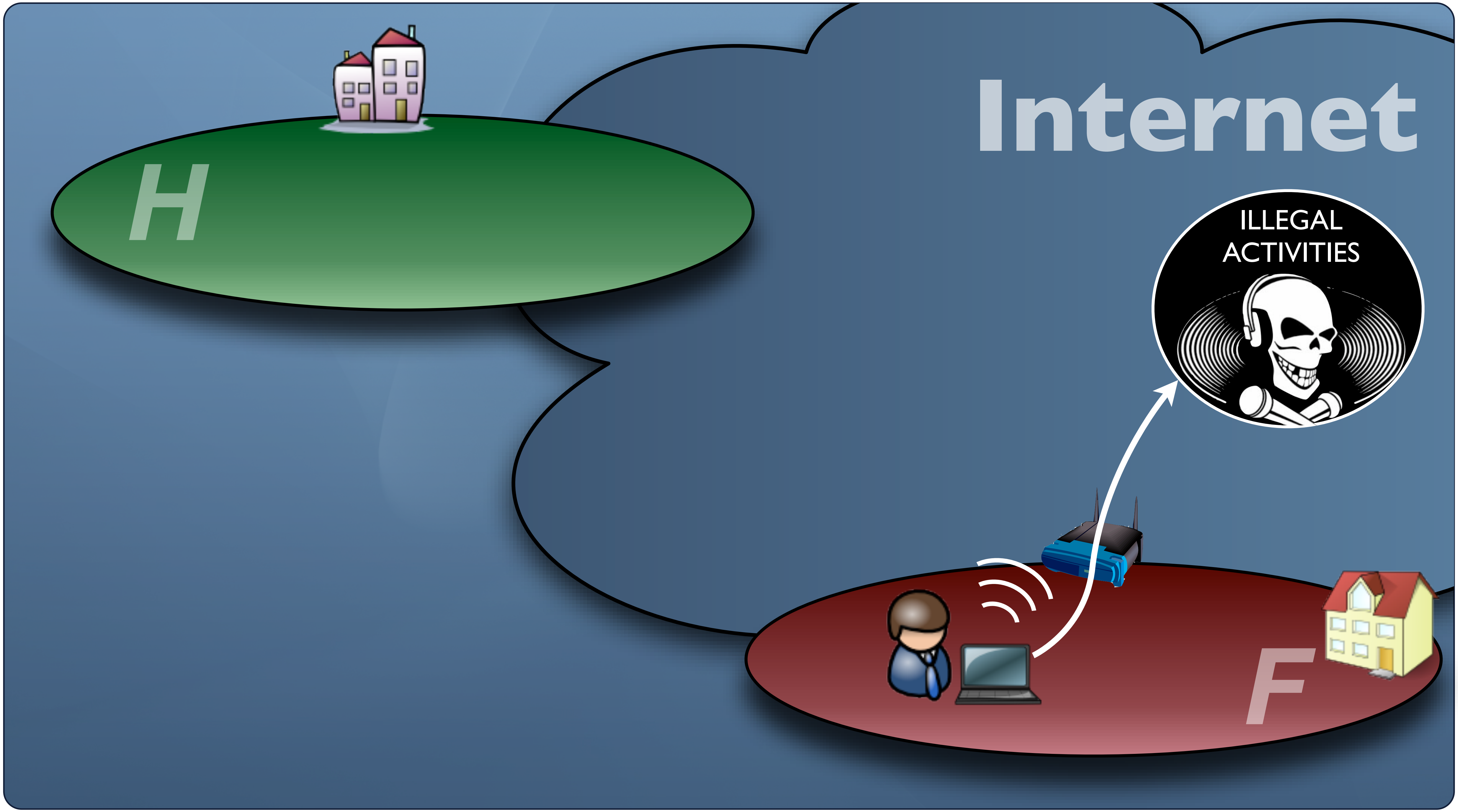
Context : Open WiFi Roaming



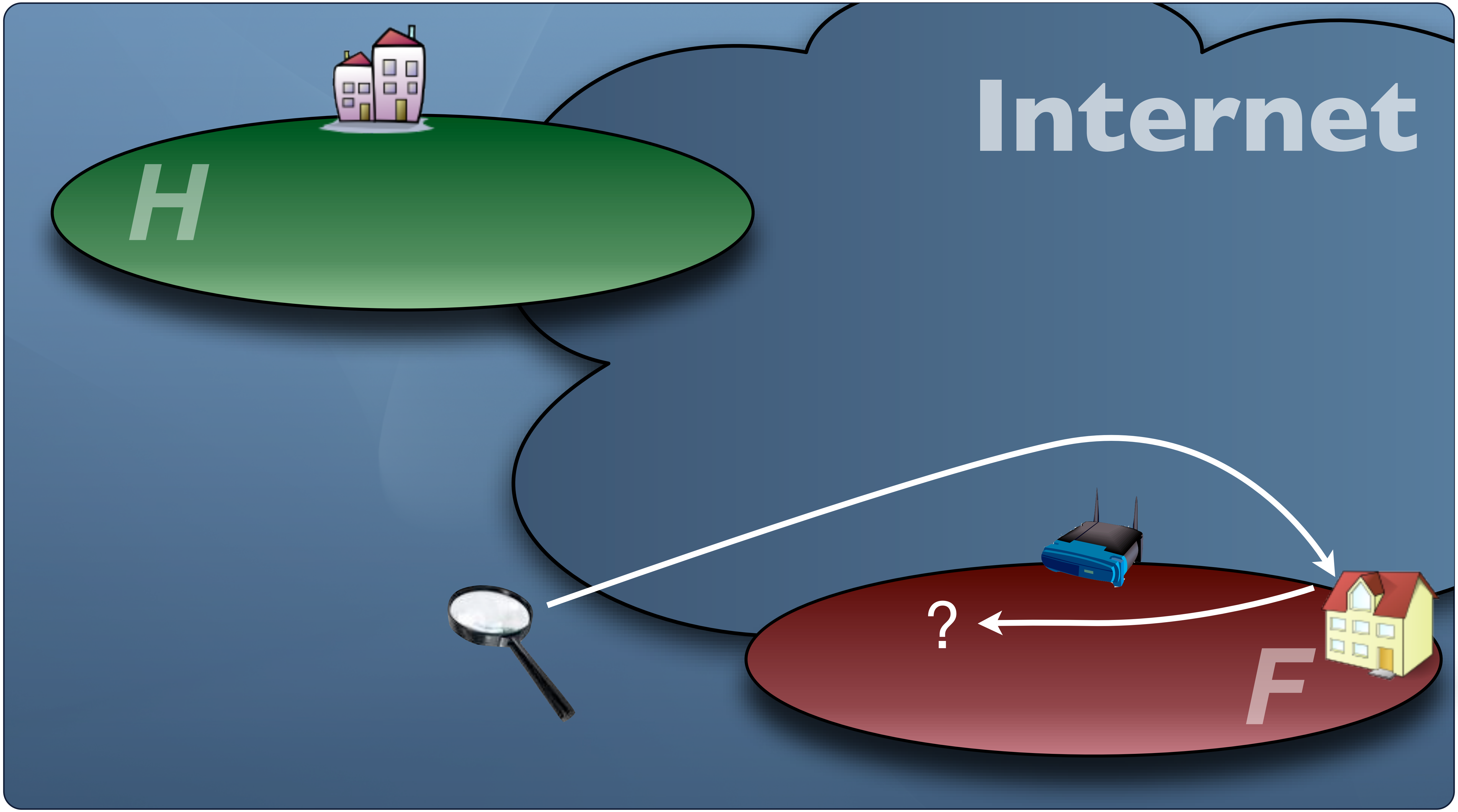
Context : Open WiFi Roaming



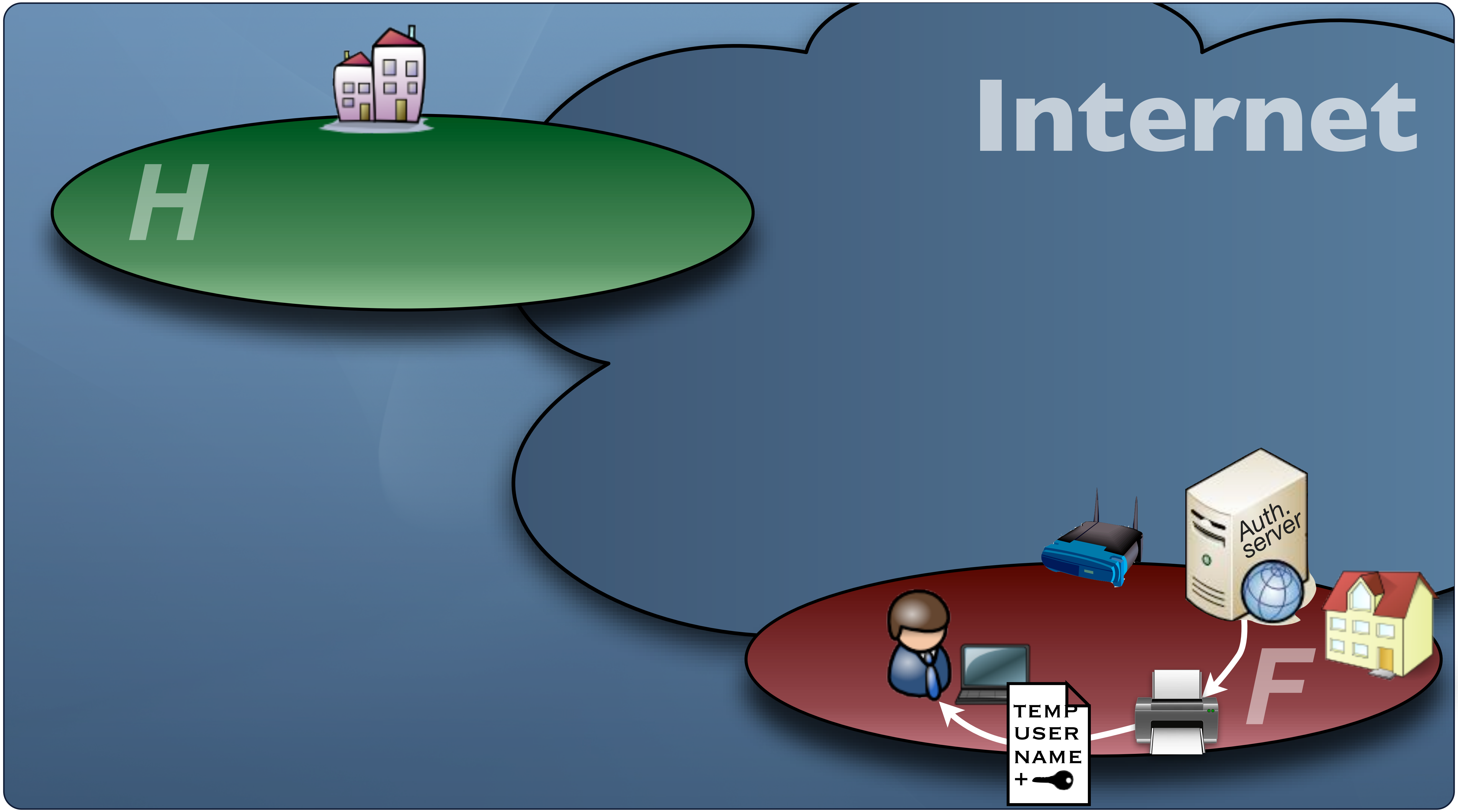
Context : Open WiFi Roaming



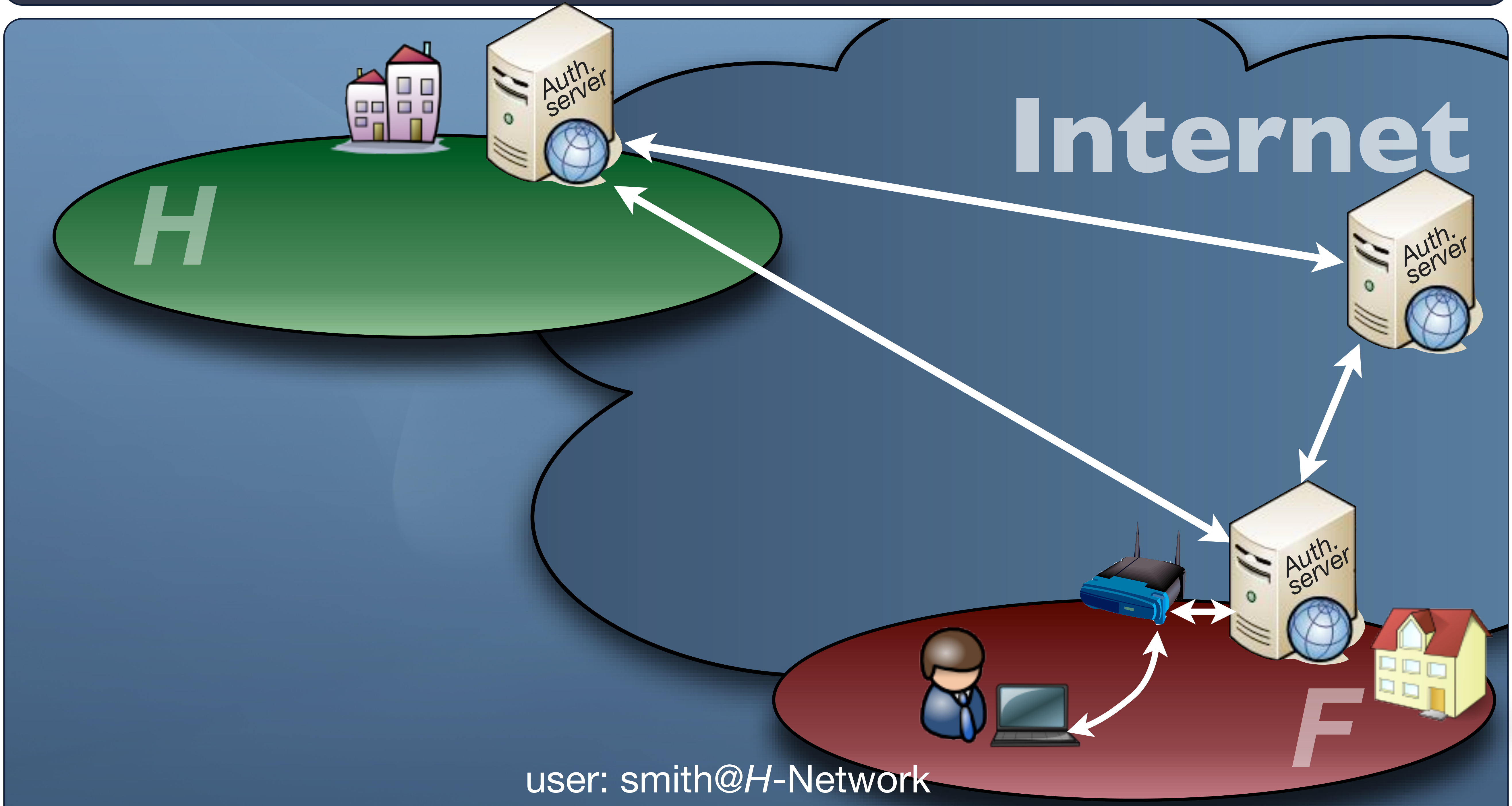
Context : Open WiFi Roaming



Context : Authenticated WiFi Roaming



Context : Authenticated WiFi Roaming

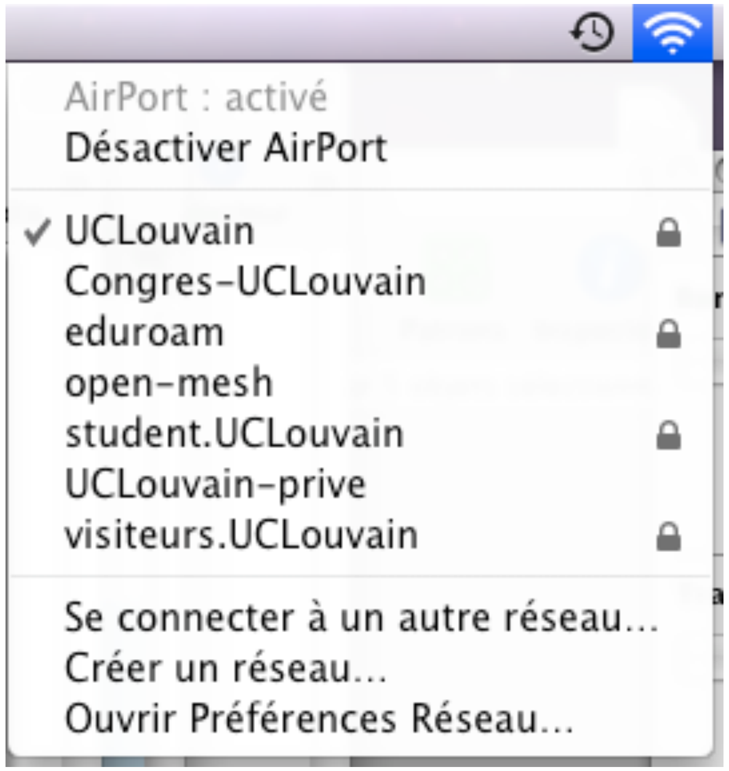


user: smith@*H*-Network

passwd : 🔑 in H

The Eduroam Project

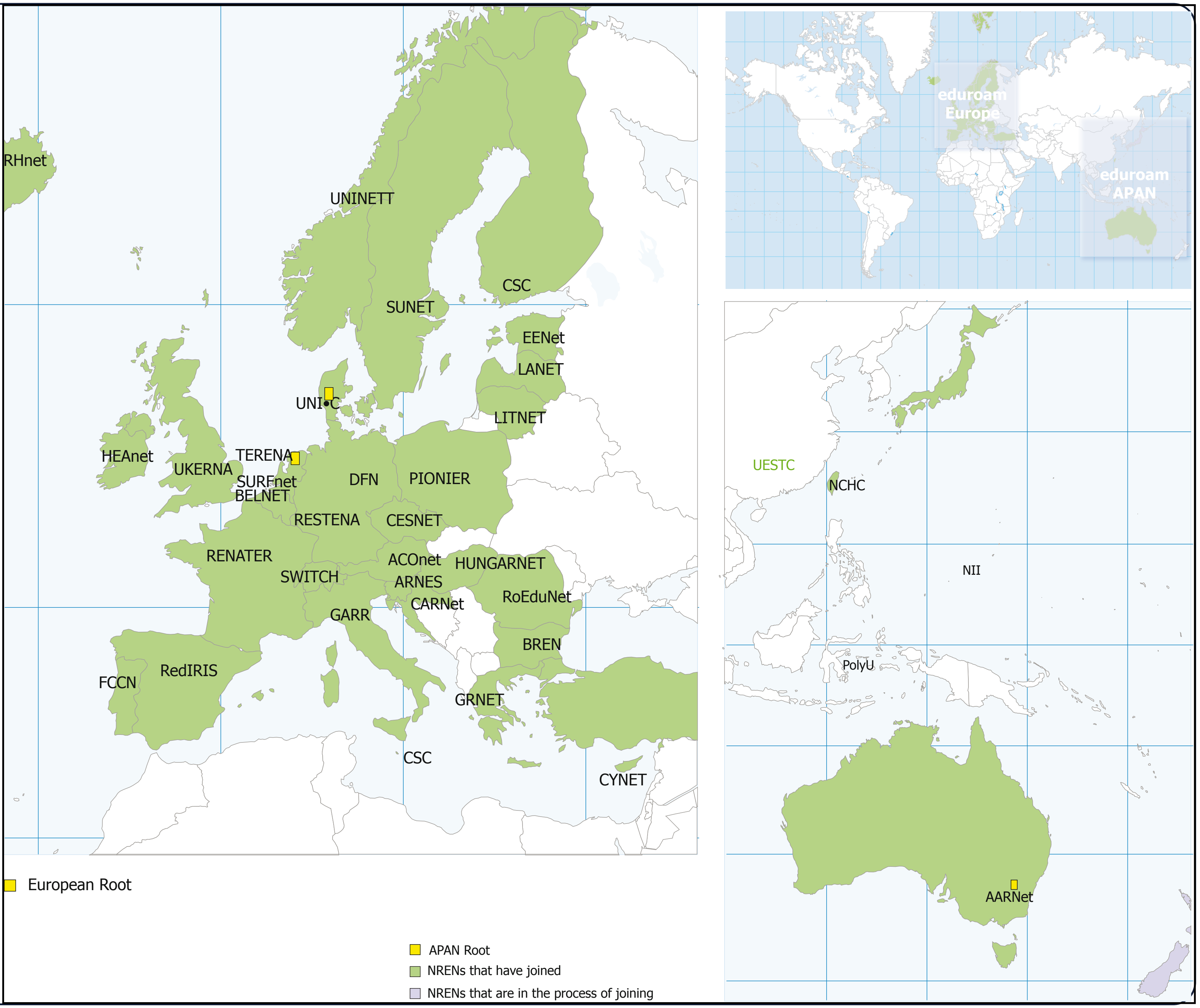
eduroam



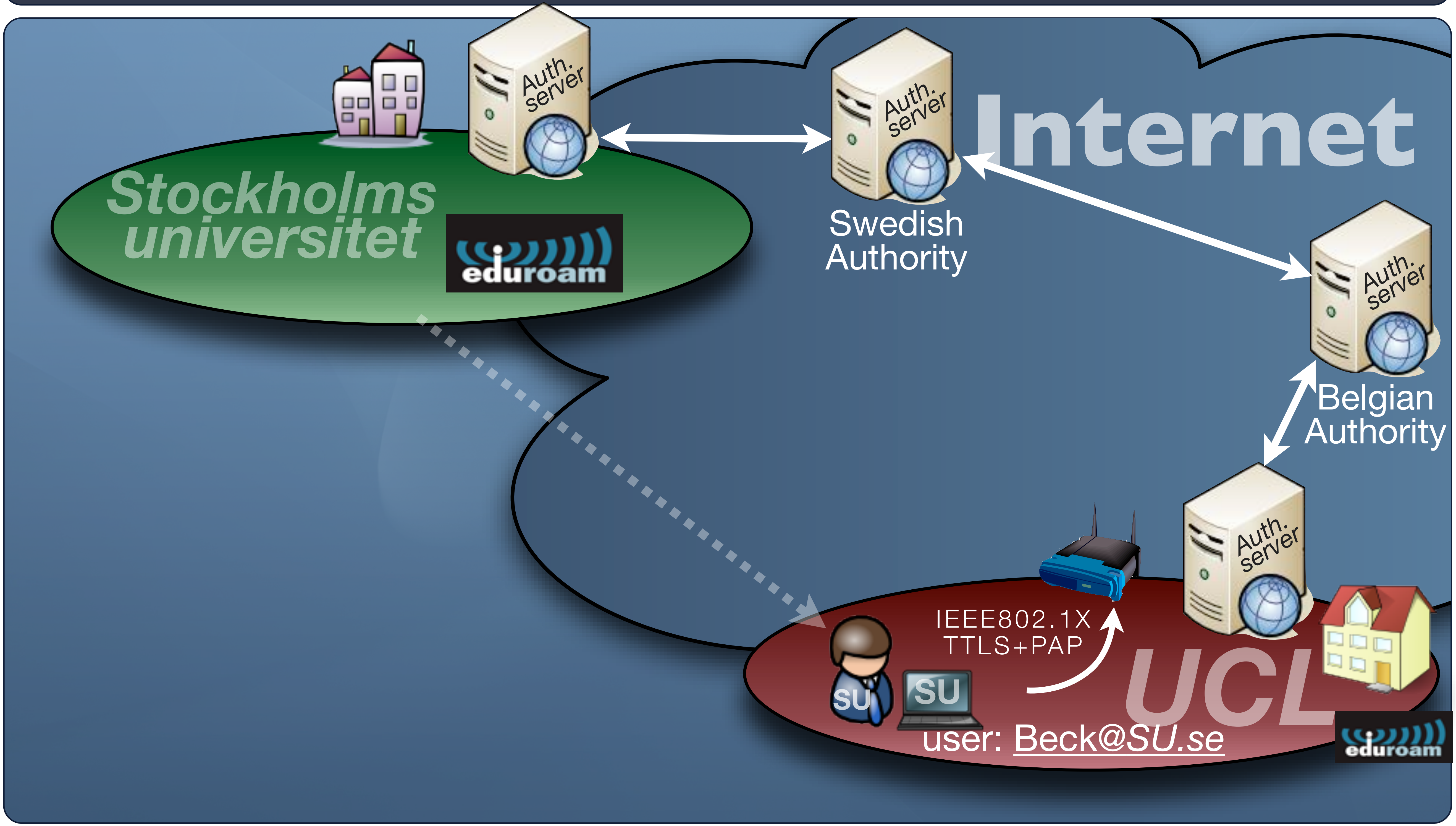
AirPort : activé
Désactiver AirPort

- ✓ UCLouvain 🔒
- Congres-UCLouvain
- eduroam 🔒
- open-mesh
- student.UCLouvain 🔒
- UCLouvain-prive
- visiteurs.UCLouvain 🔒

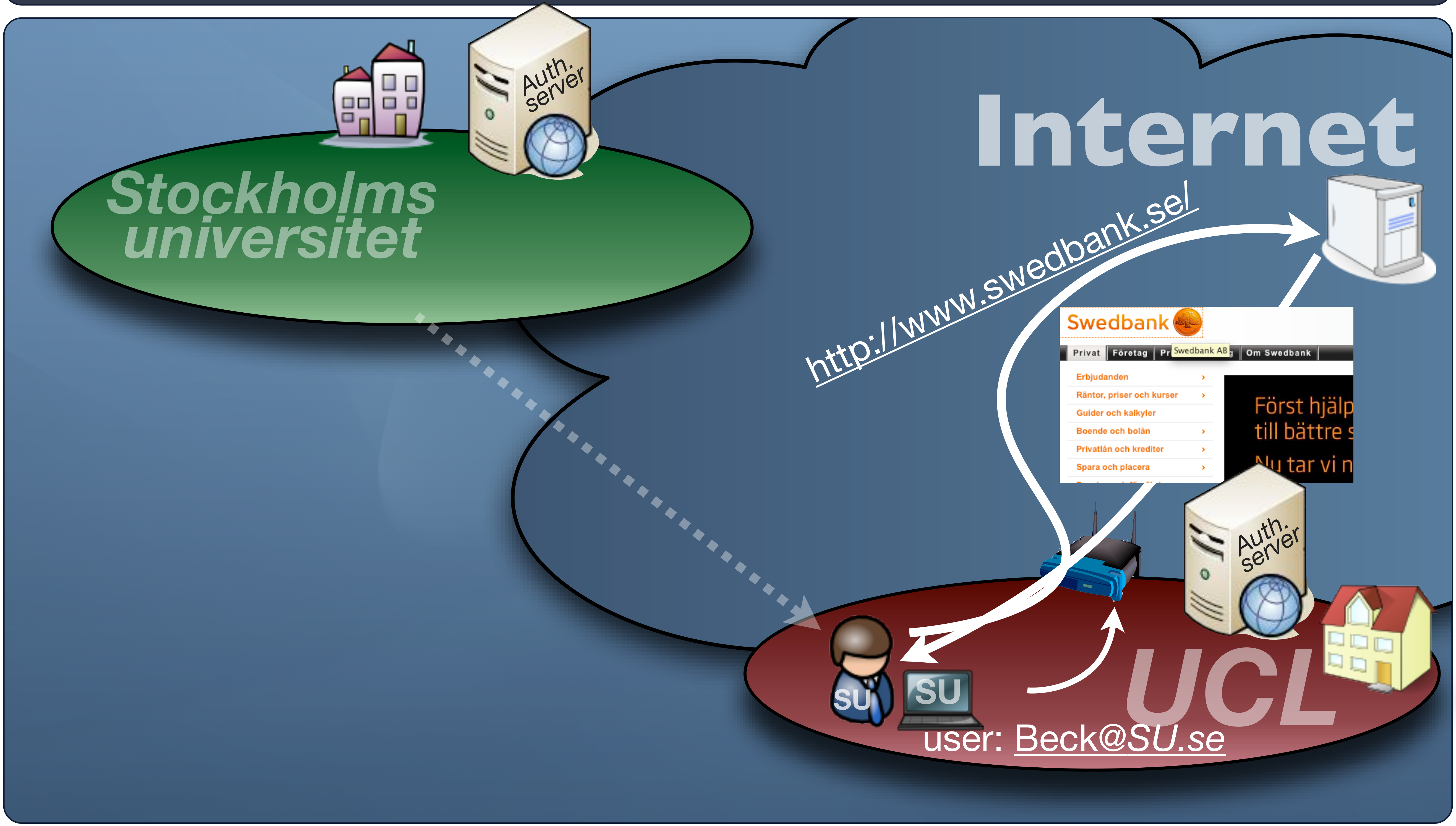
Se connecter à un autre réseau…
Créer un réseau…
Ouvrir Préférences Réseau…



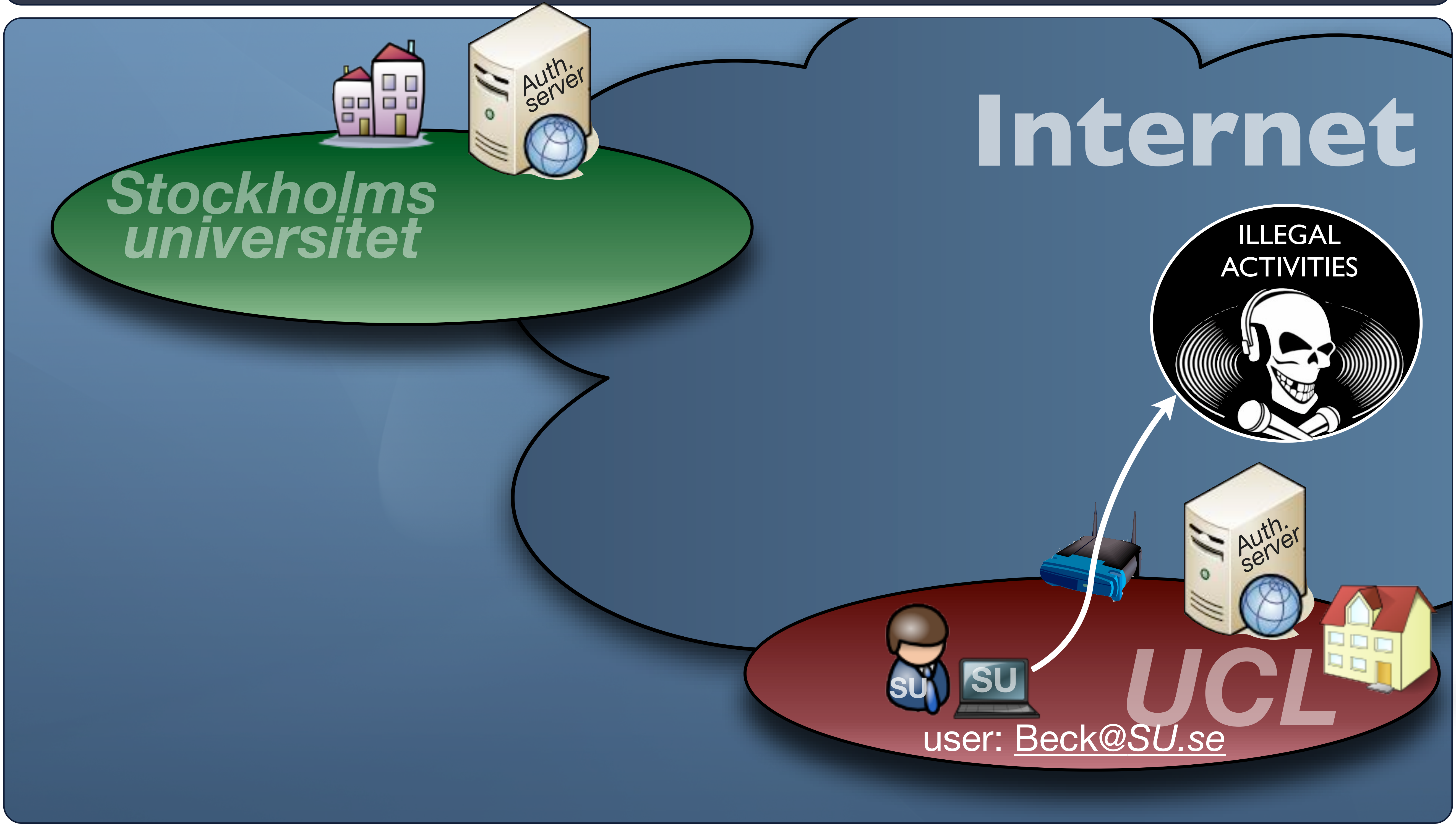
Roaming with Eduroam



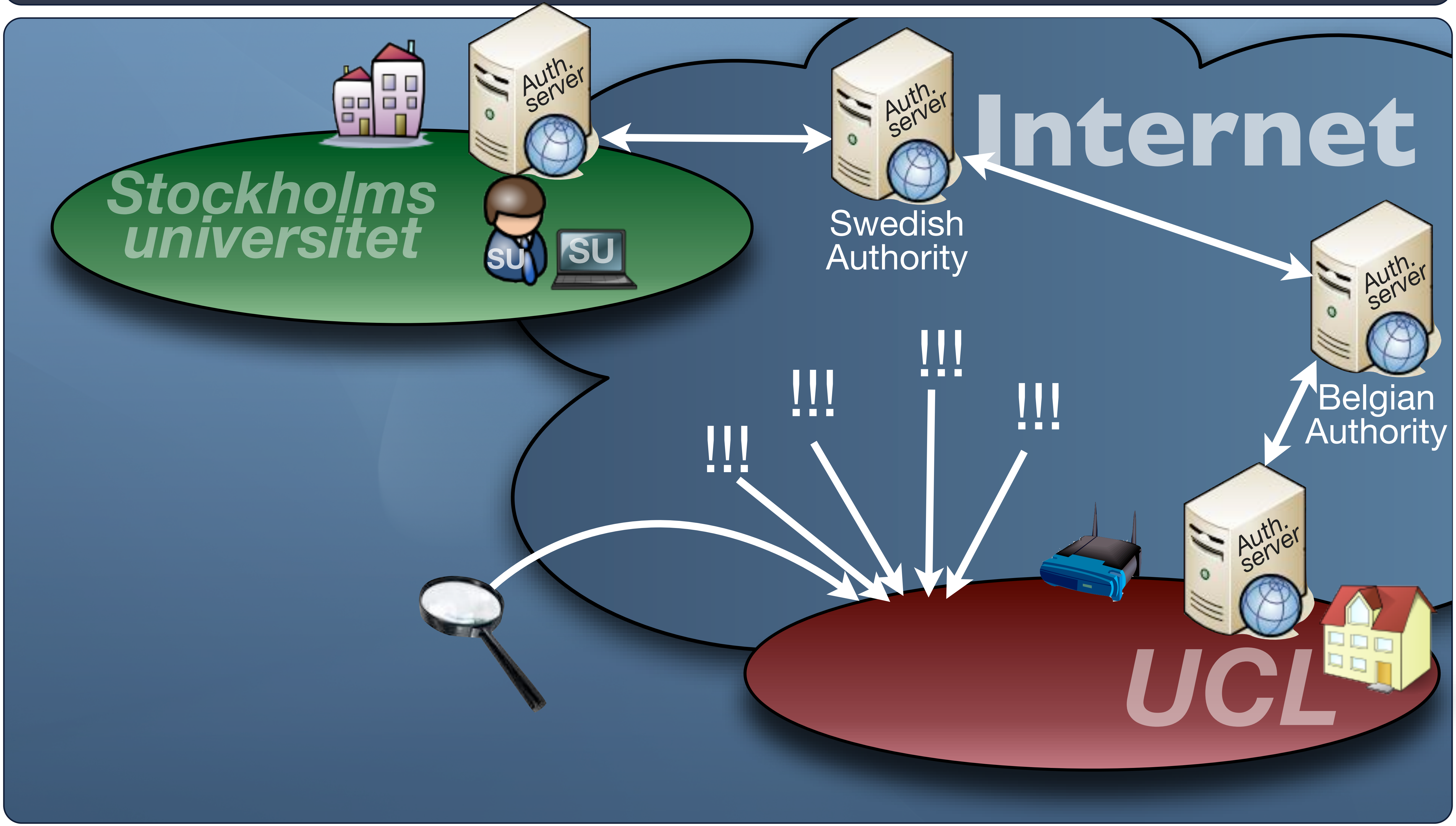
Roaming with Eduroam



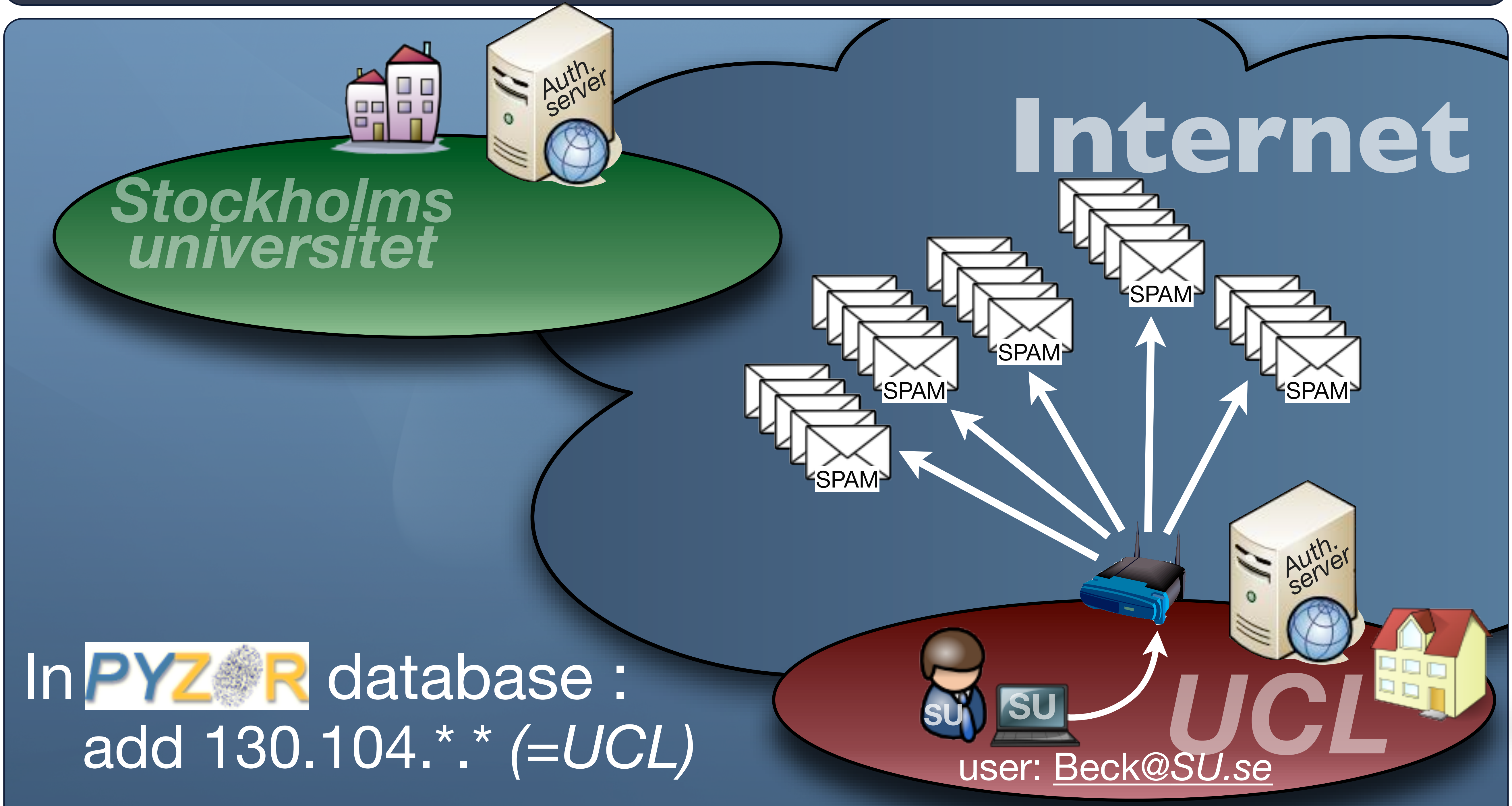
Eduroam - Client abuse scenario



Eduroam - Client abuse scenario

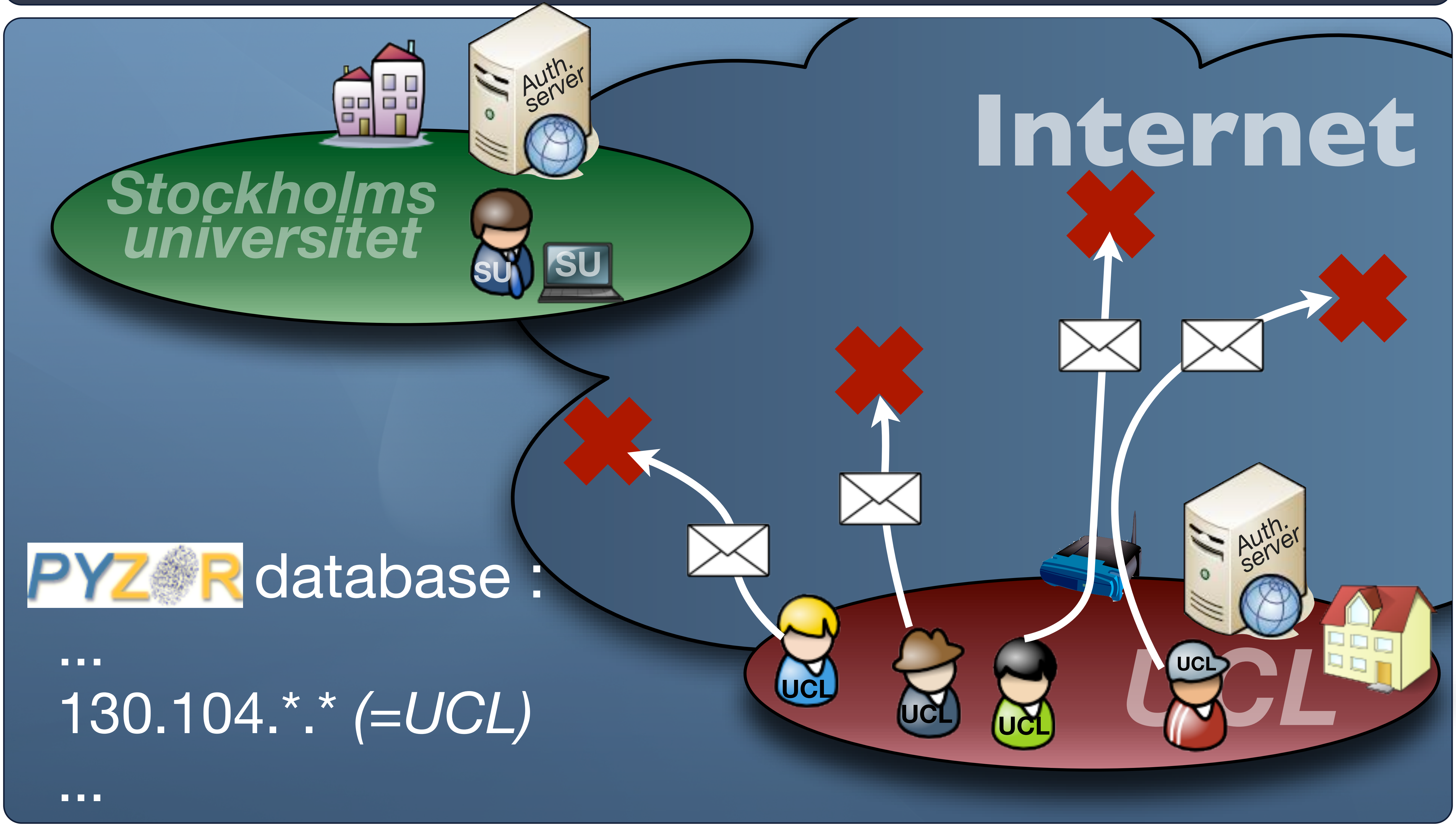


Eduroam - Client abuse scenario



In PYZOR database :
add 130.104.*.* *(=UCL)*

Eduroam - Client abuse scenario



PYZOR database :

...

130.104.*.* *(=UCL)*

...

Potential Security Risks

Malicious F (Foreign network)

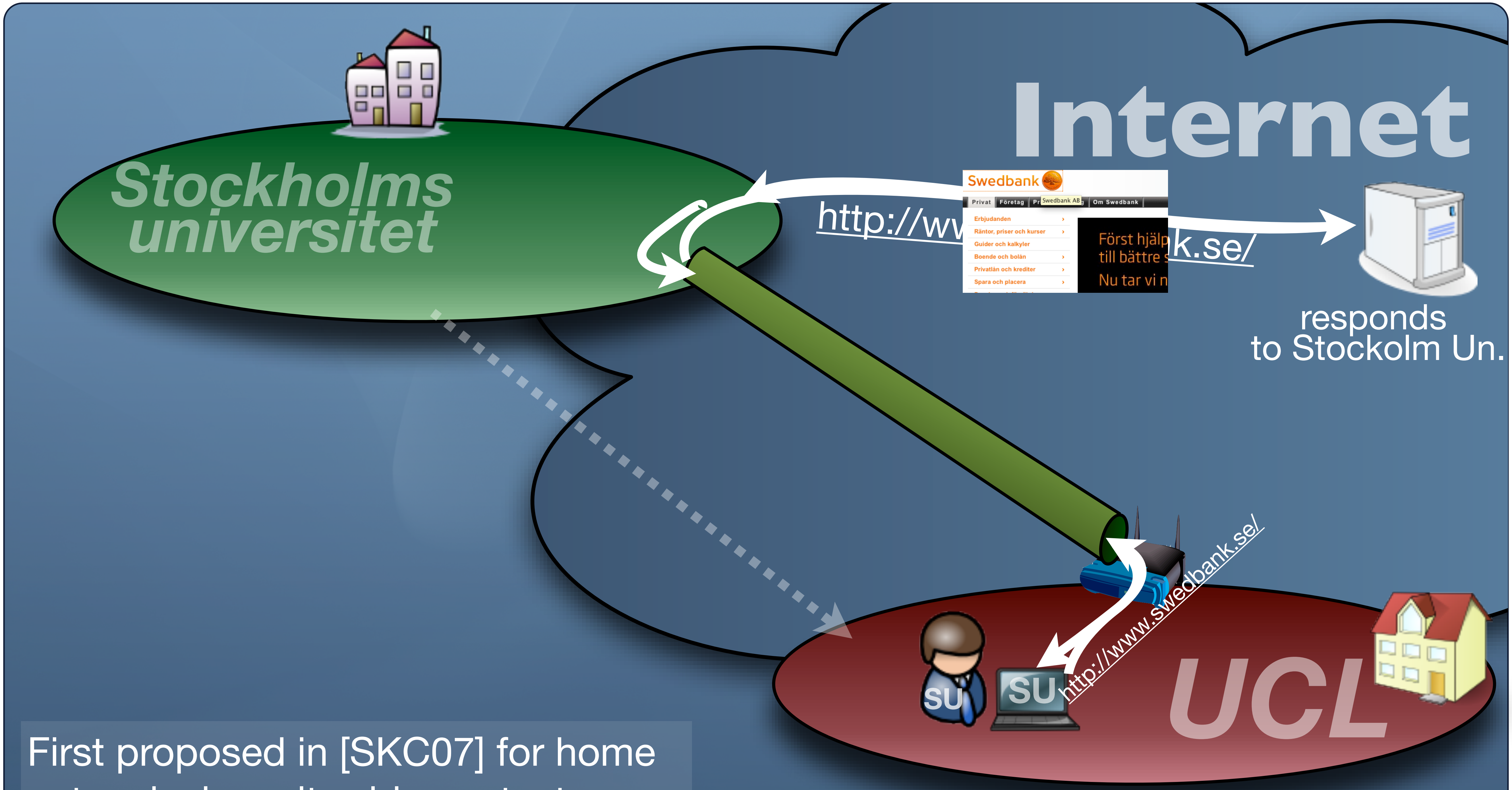
- DNS manipulations (i.e., pharming)
- Stealing credentials
- Sniffing
- Claim higher cost

Potential Security Risks

Malicious M (Mobile node)

- Misbehavior on the Internet using IP of F
- Risk for infrastructure of F (attack easier from the inside)
- Access control based on IP (intranet, digital libraries, ...)

Wireless Roaming via Tunnels (WRT)



First proposed in [SKC07] for home networks in a citywide context

Wireless Roaming via Tunnels (WRT)

Advantages

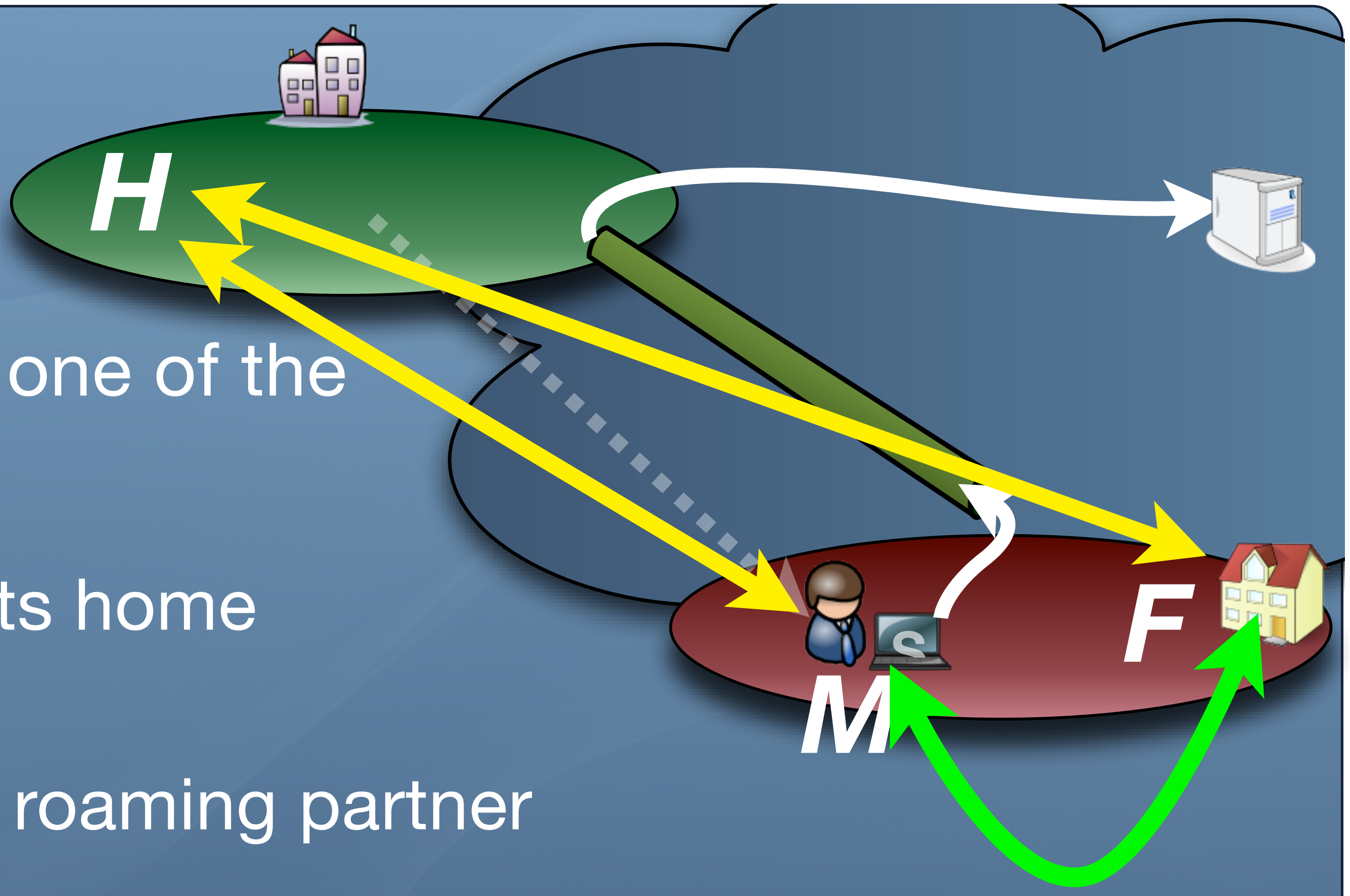
- ✓ If the user sends spam, SU is blamed (and blacklisted), not UCL
- ✓ UCL does not care about SU user activities !
- ✓ Traffic from Beck to SU can be encrypted (= hidden from UCL)
- ✓ Cost based on traffic can be measured by H

AWRT

- = Authentication and Key Establishment Protocol for Wireless Roaming via Tunnels
- Formal security model (in the paper)
- A protocol (in the next slides)
- + proofs (on authors’ website)

Security Goals

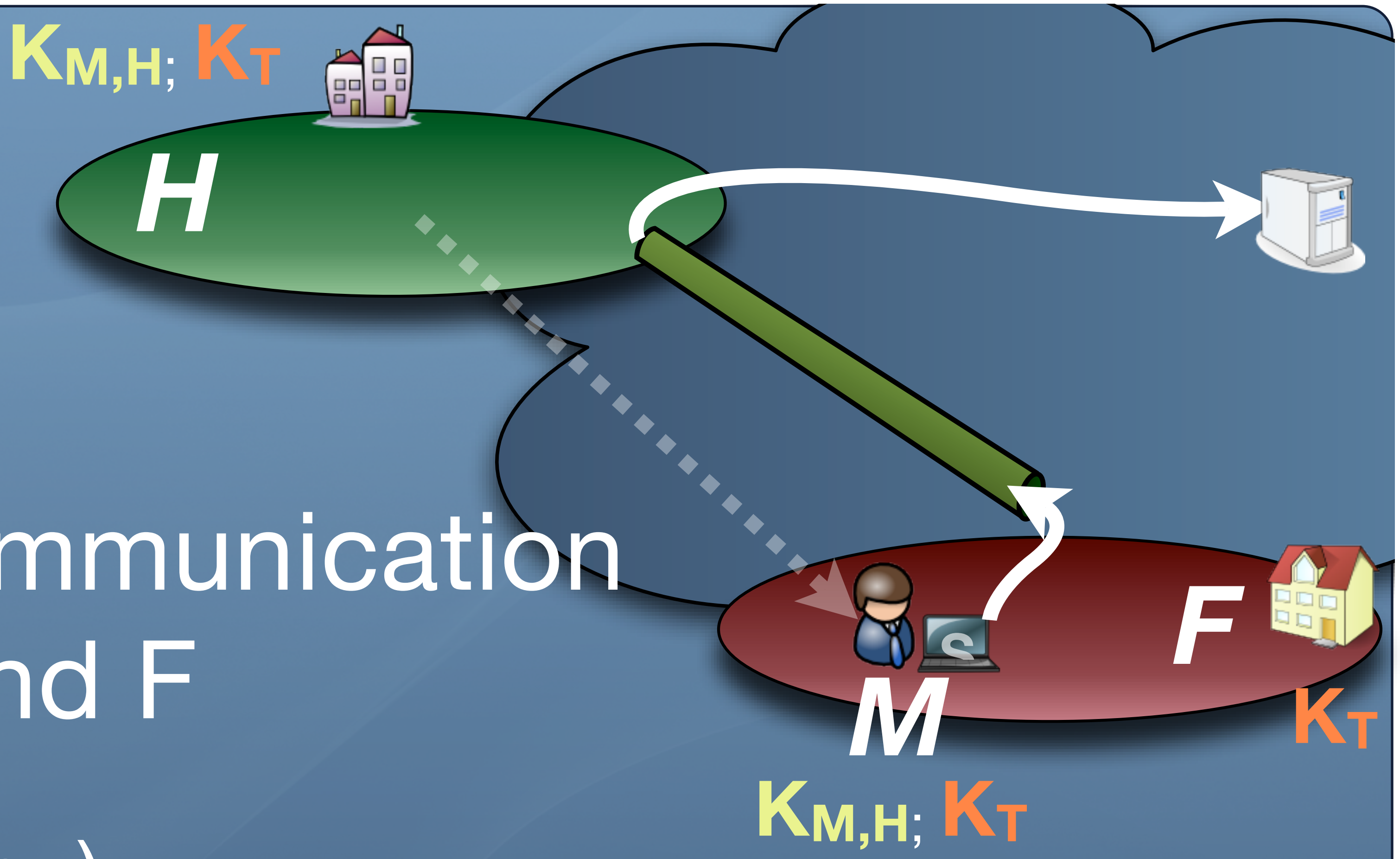
Authentication



- H must authenticate M as one of the registered mobile devices
- M must authenticate H as its home network
- F must authenticate H as a roaming partner
- H must authenticate F as a roaming partner
- F trusts H to correctly authenticate M
- M trusts H to correctly authenticate F

Security Goals

Key establishment



- Protection of communication between M, H and F
  - ➡ K_T (tunnel key)
- End-to-end protection
  - ➡ $K_{M,H}$ (end-to-end key)

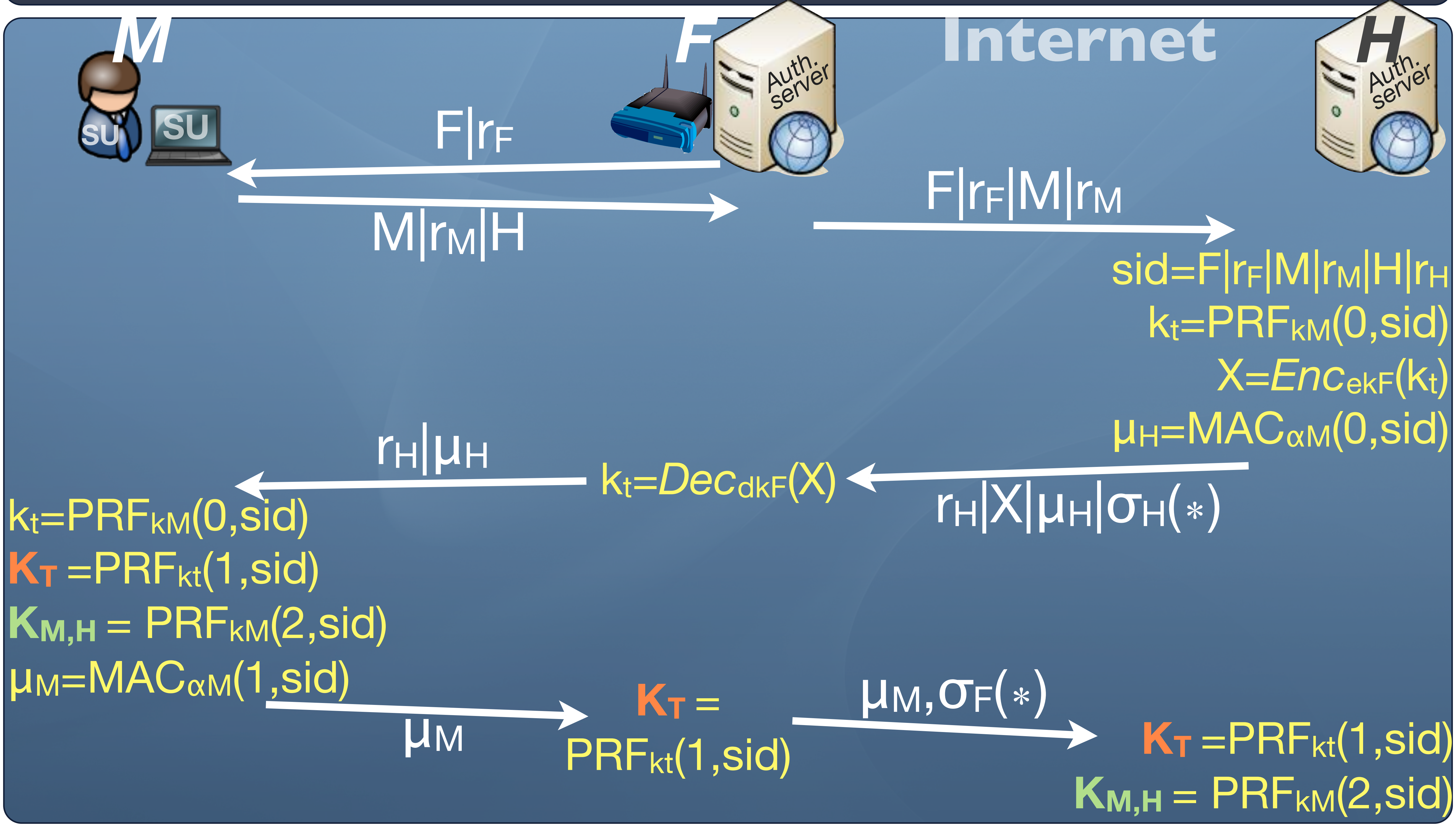
Building Blocks

- PRF (pseudo-random function) $\{0,1\}^{\kappa} \times \{0,1\}^{*} \rightarrow \{0,1\}^{n}$
    - Used for key derivation
- Asymmetric encryption scheme (with IND-CCA2 property) (functions ***Enc*** and ***Dec***)
- Digital signature scheme (with EUF-CMA property) (functions ***Sig*** and ***Ver***)
- MAC (Message Authentication Code) (with WUF-CMA property)

AWRT - Initialization

- F is in possession of :
  - (dk_F, ek_F), (sk_F, vk_F)
  - $(H, vk_H)_j$ for each roaming partner *j*
- H is in possession of :
  - (sk_M, vk_M)
  - $(M, k_M, \alpha_M)_i$ for each mobile *i* user of H
  - $(F, vk_F, dk_F)_j$ for each roaming partner *j*
- M is in possession of :
  - k_M, α_M

AWRT - The protocol (simplified)



$F|r_F$

$M|r_M|H$

$F|r_F|M|r_M$

$sid=F|r_F|M|r_M|H|r_H$
$k_t=PRF_{kM}(0,sid)$
$X=\mathit{Enc}_{ekF}(k_t)$
$\mu_H=MAC_{\alpha M}(0,sid)$

$r_H|X|\mu_H|\sigma_H(*)$

$k_t=\mathit{Dec}_{dkF}(X)$

$r_H|\mu_H$

$k_t=PRF_{kM}(0,sid)$
$\mathbf{K_T}=PRF_{kt}(1,sid)$
$\mathbf{K_{M,H}}=PRF_{kM}(2,sid)$
$\mu_M=MAC_{\alpha M}(1,sid)$

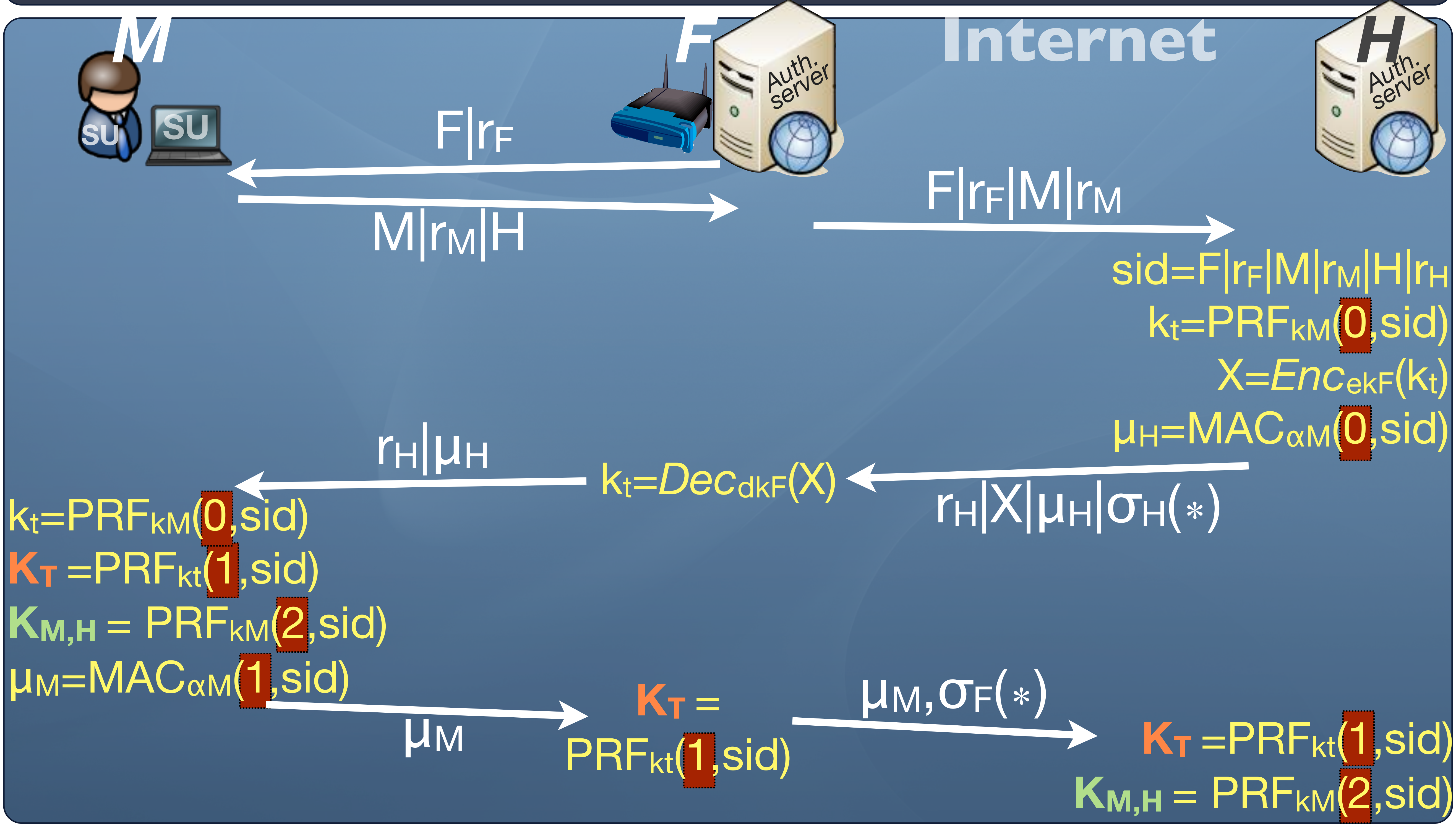
μ_M

$\mathbf{K_T}=PRF_{kt}(1,sid)$

$\mu_M,\sigma_F(*)$

$\mathbf{K_T}=PRF_{kt}(1,sid)$
$\mathbf{K_{M,H}}=PRF_{kM}(2,sid)$

AWRT - The protocol (simplified)



$F|r_F$

$M|r_M|H$

$F|r_F|M|r_M$

$sid=F|r_F|M|r_M|H|r_H$

$k_t=PRF_{kM}(0,sid)$

$X=\mathit{Enc}_{ekF}(k_t)$

$\mu_H=MAC_{\alpha M}(0,sid)$

$r_H|\mu_H$

$k_t=\mathit{Dec}_{dkF}(X)$

$r_H|X|\mu_H|\sigma_H(*)$

$k_t=PRF_{kM}(0,sid)$

$K_T=PRF_{kt}(1,sid)$

$K_{M,H}=PRF_{kM}(2,sid)$

$\mu_M=MAC_{\alpha M}(1,sid)$

μ_M

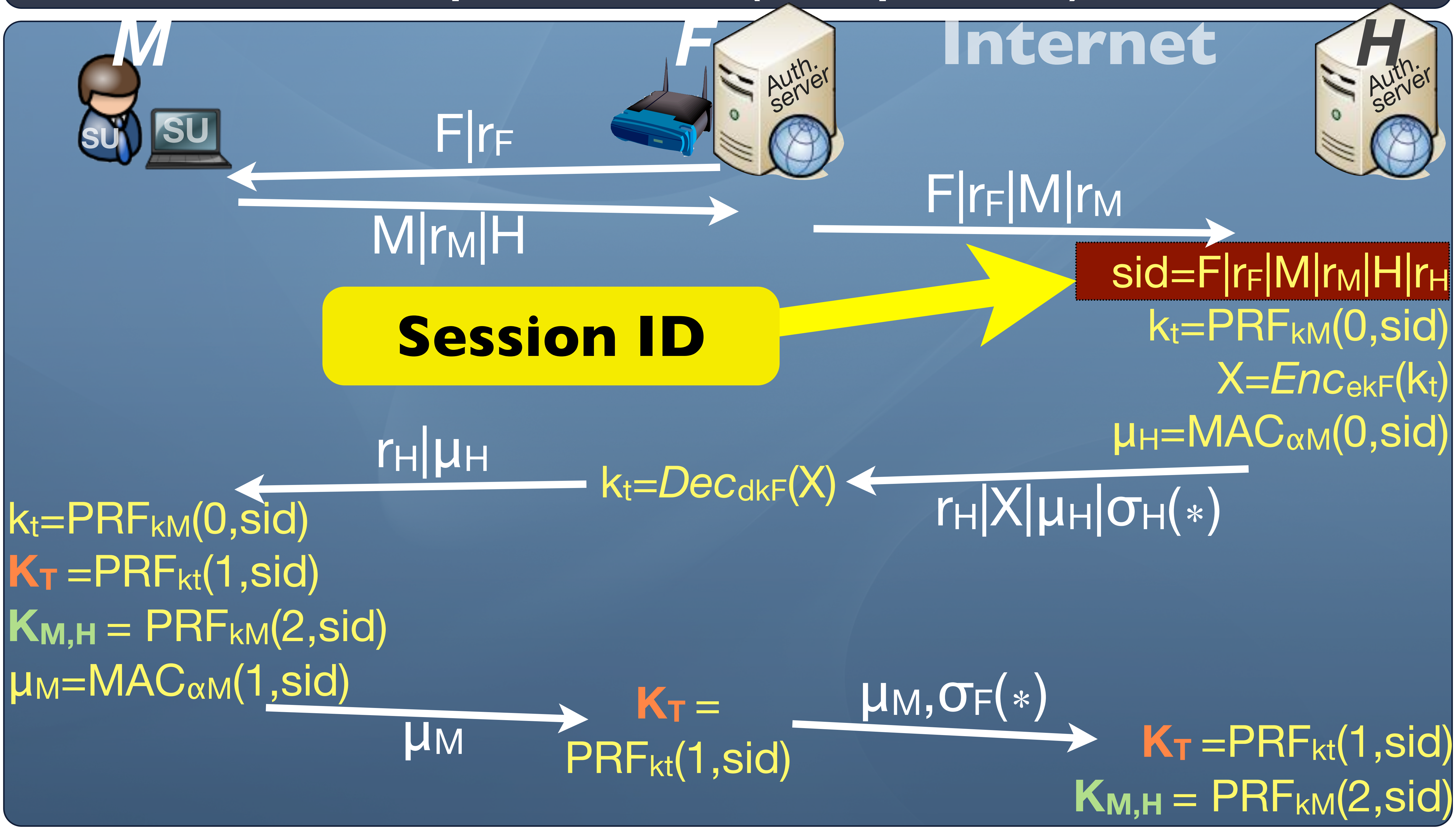
$K_T=PRF_{kt}(1,sid)$

$\mu_M,\sigma_F(*)$

$K_T=PRF_{kt}(1,sid)$

$K_{M,H}=PRF_{kM}(2,sid)$

AWRT - The protocol (simplified)



$F|r_F$

$M|r_M|H$

$F|r_F|M|r_M$

Session ID

$sid=F|r_F|M|r_M|H|r_H$

$k_t=PRF_{kM}(0,sid)$

$X=Enc_{ekF}(k_t)$

$\mu_H=MAC_{\alpha M}(0,sid)$

$r_H|X|\mu_H|\sigma_H(*)$

$k_t=Dec_{dkF}(X)$

$r_H|\mu_H$

$k_t=PRF_{kM}(0,sid)$

$K_T=PRF_{kt}(1,sid)$

$K_{M,H}=PRF_{kM}(2,sid)$

$\mu_M=MAC_{\alpha M}(1,sid)$

μ_M

$K_T=PRF_{kt}(1,sid)$

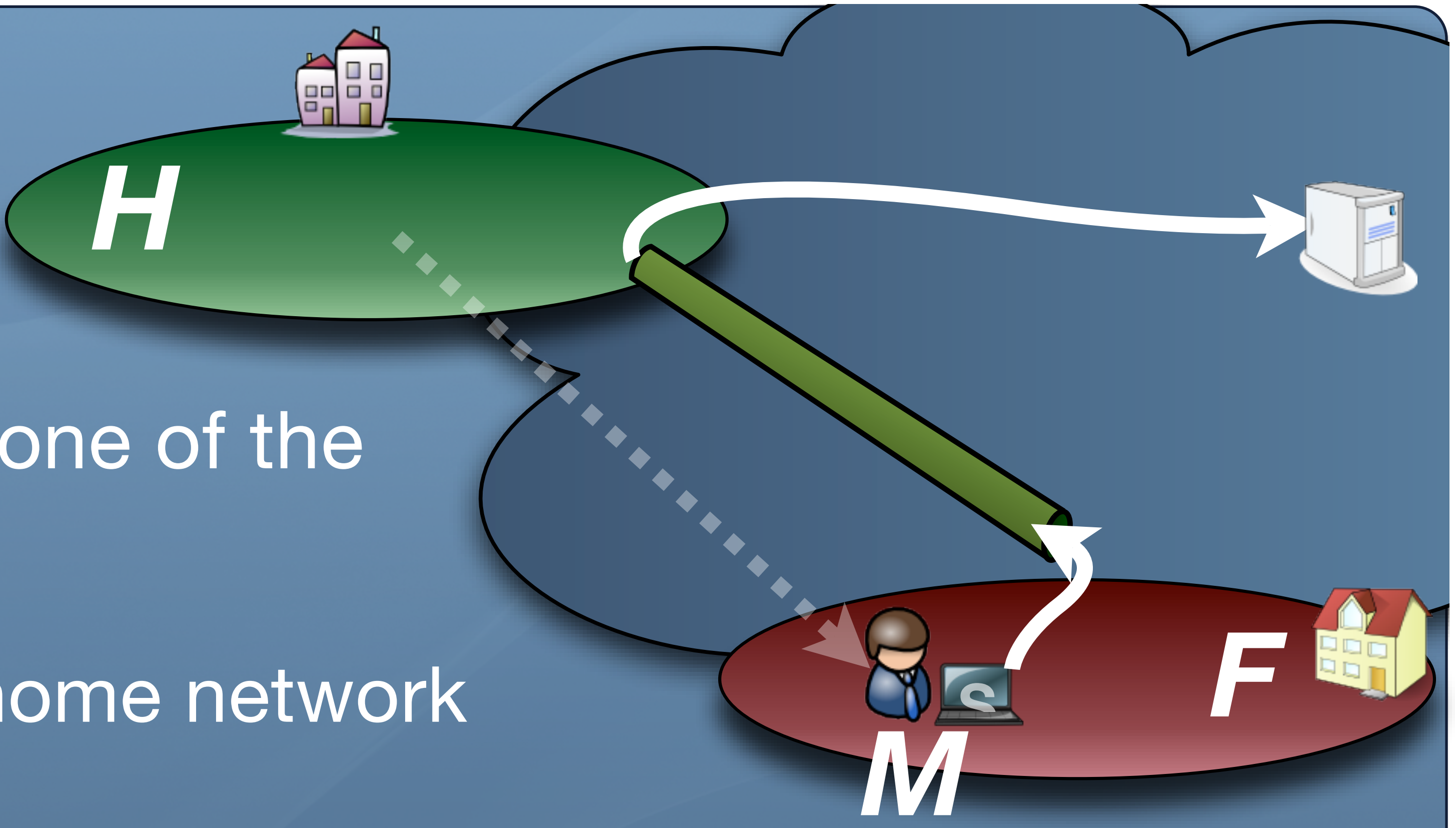
$\mu_M,\sigma_F(*)$

$K_T=PRF_{kt}(1,sid)$

$K_{M,H}=PRF_{kM}(2,sid)$

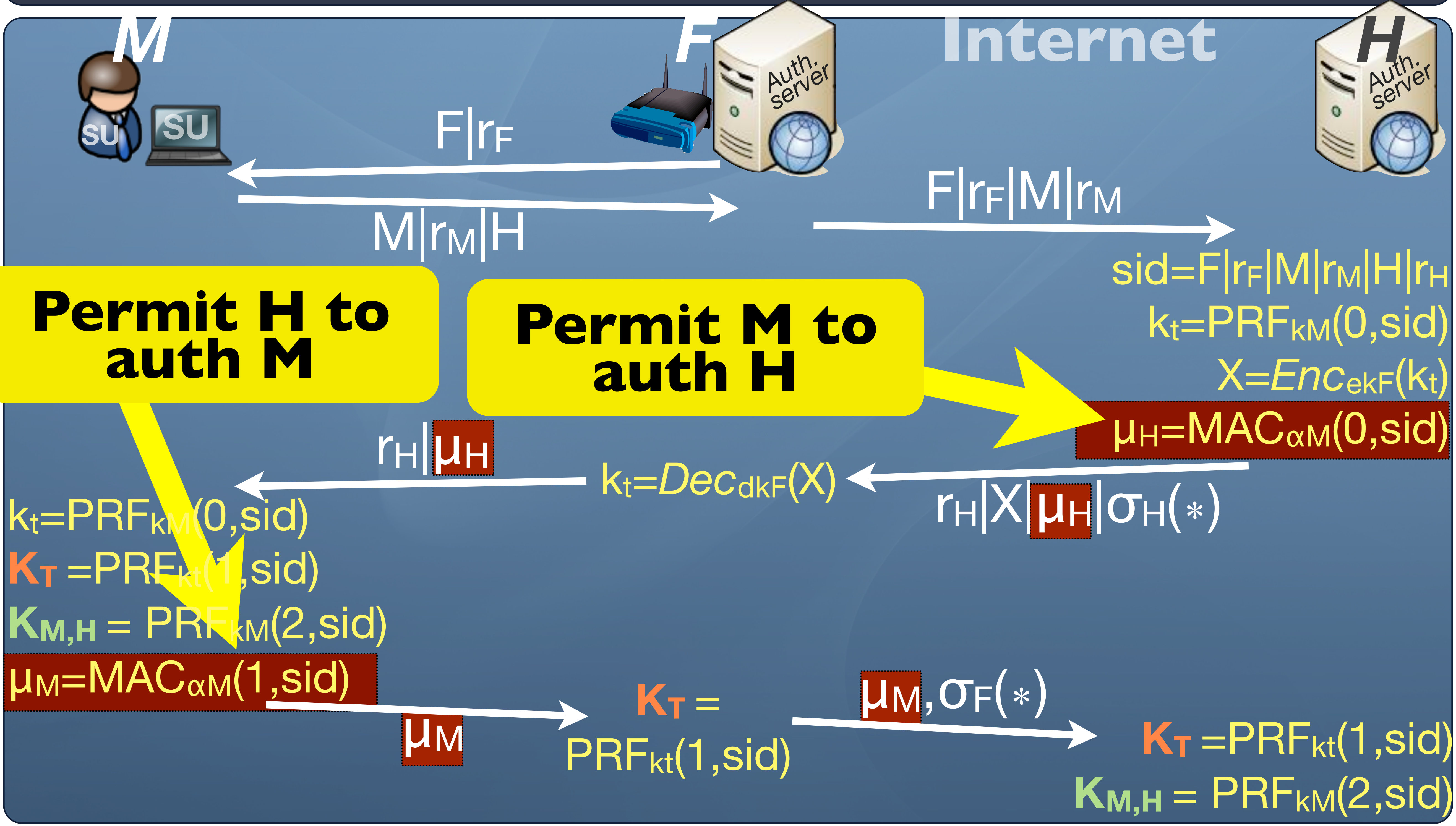
Security Goals

Authentication



- H must authenticate M as one of the registered mobile devices
- M must authenticate H as home network
- F must authenticate H as a roaming partner
- H must authenticate F as a roaming parter
- F trusts H to correctly authenticate M
- M trusts H to correctly authenticate F

AWRT - The protocol (simplified)



$F|r_F$

$M|r_M|H$

$F|r_F|M|r_M$

$sid=F|r_F|M|r_M|H|r_H$

$k_t=PRF_{kM}(0,sid)$

$X=Enc_{ekF}(k_t)$

$\mu_H=MAC_{\alpha M}(0,sid)$

Permit H to auth M

Permit M to auth H

$r_H|X|\mu_H|\sigma_H(*)$

$k_t=Dec_{dkF}(X)$

$r_H|\mu_H$

$k_t=PRF_{kM}(0,sid)$

$K_T=PRF_{kt}(1,sid)$

$K_{M,H} = PRF_{kM}(2,sid)$

$\mu_M=MAC_{\alpha M}(1,sid)$

μ_M

$K_T = PRF_{kt}(1,sid)$

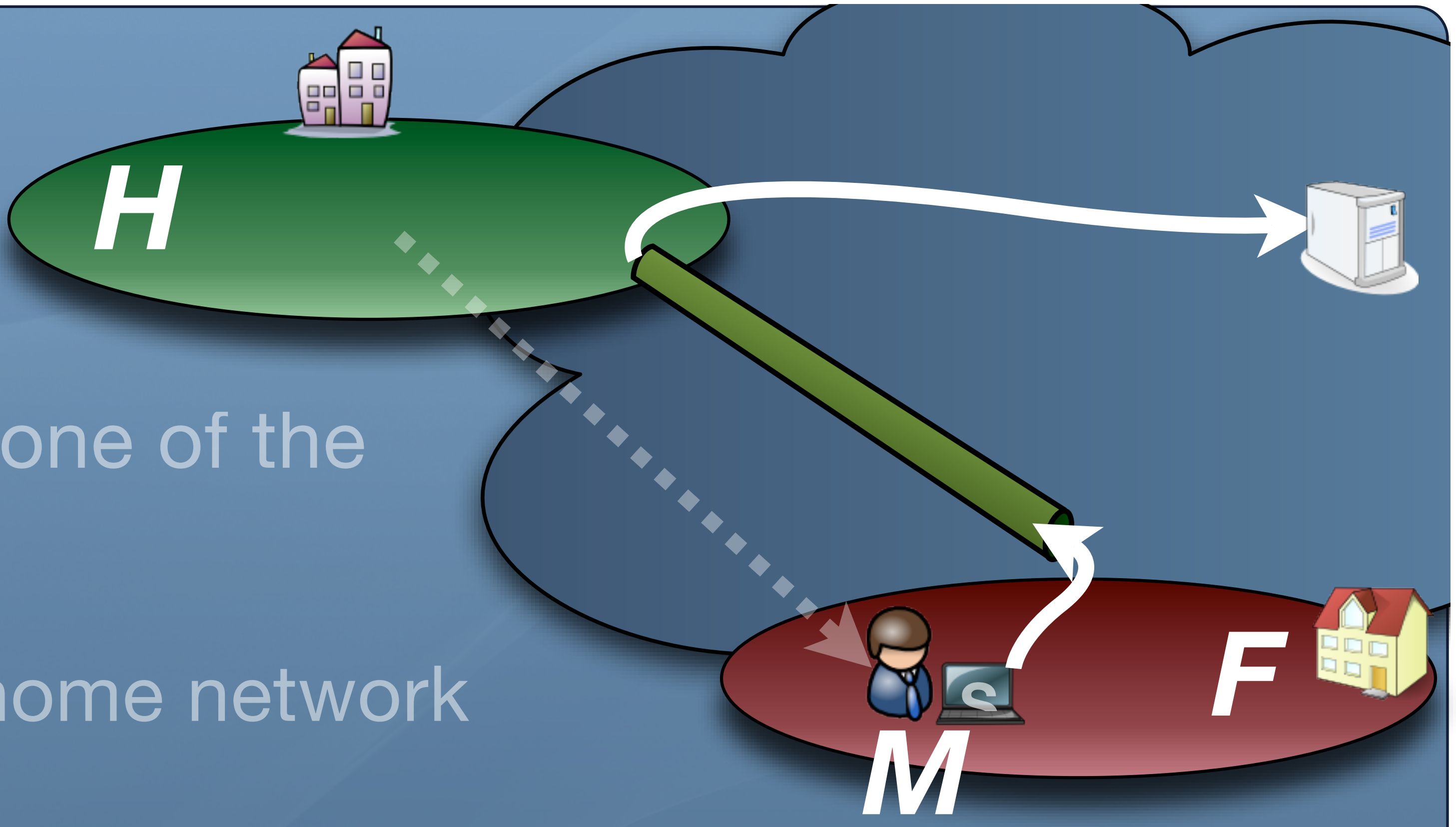
$\mu_M,\sigma_F(*)$

$K_T=PRF_{kt}(1,sid)$

$K_{M,H} = PRF_{kM}(2,sid)$

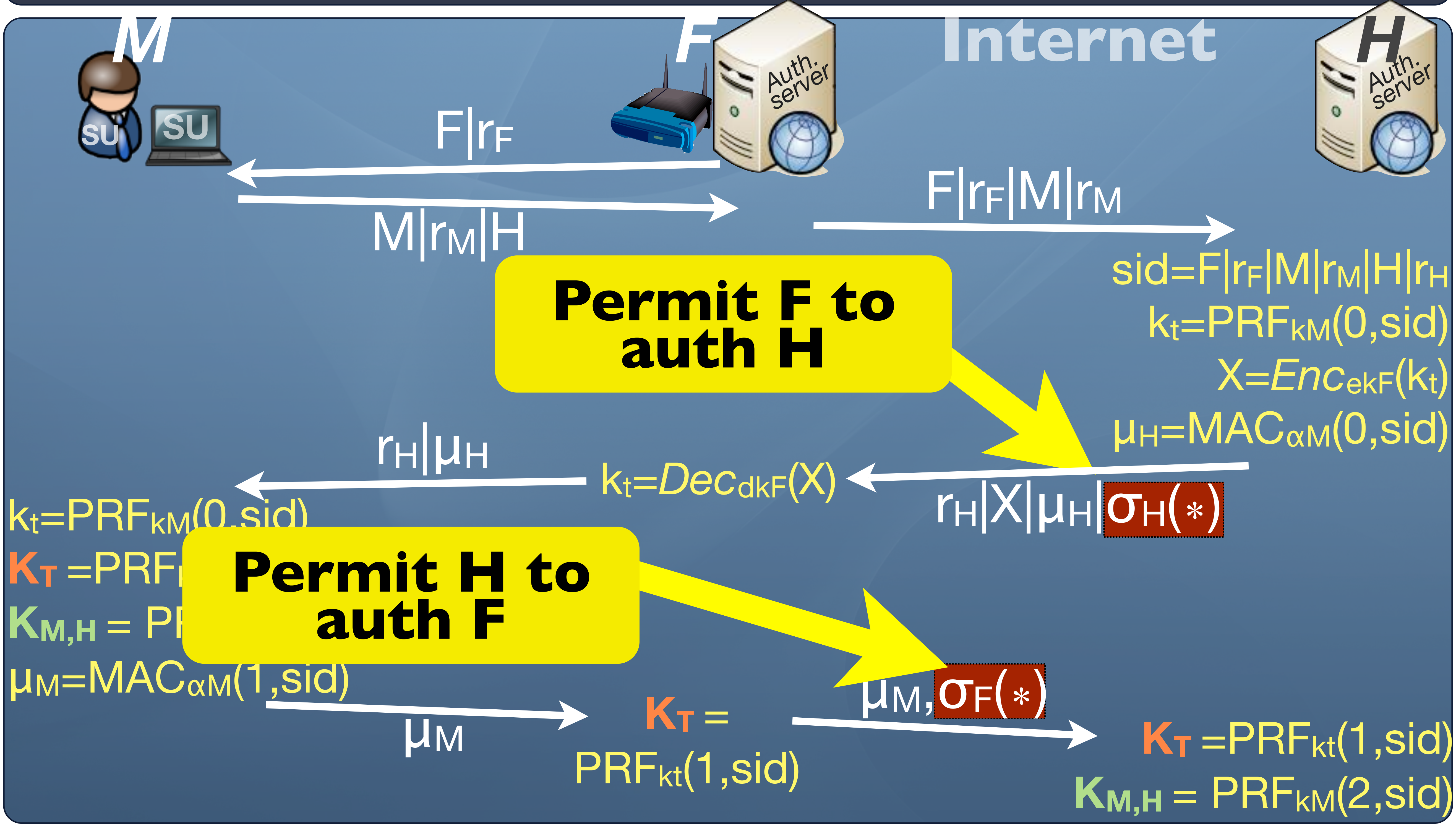
Security Goals

Authentication



- H must authenticate M as one of the registered mobile devices
- M must authenticate H as home network
- F must authenticate H as a roaming partner
- H must authenticate F as a roaming parter
- F trusts H to correctly authenticate M
- M trusts H to correctly authenticate F

AWRT - The protocol (simplified)



$F|r_F$

$M|r_M|H$

$F|r_F|M|r_M$

$sid=F|r_F|M|r_M|H|r_H$

$k_t=PRF_{kM}(0,sid)$

$X=Enc_{ekF}(k_t)$

$\mu_H=MAC_{\alpha M}(0,sid)$

Permit F to auth H

$r_H|X|\mu_H|\sigma_H(*)$

$k_t=Dec_{dkF}(X)$

$r_H|\mu_H$

$k_t=PRF_{kM}(0,sid)$

$K_T =PRF$

$K_{M,H} = P$

$\mu_M=MAC_{\alpha M}(1,sid)$

Permit H to auth F

μ_M

$K_T = PRF_{kt}(1,sid)$

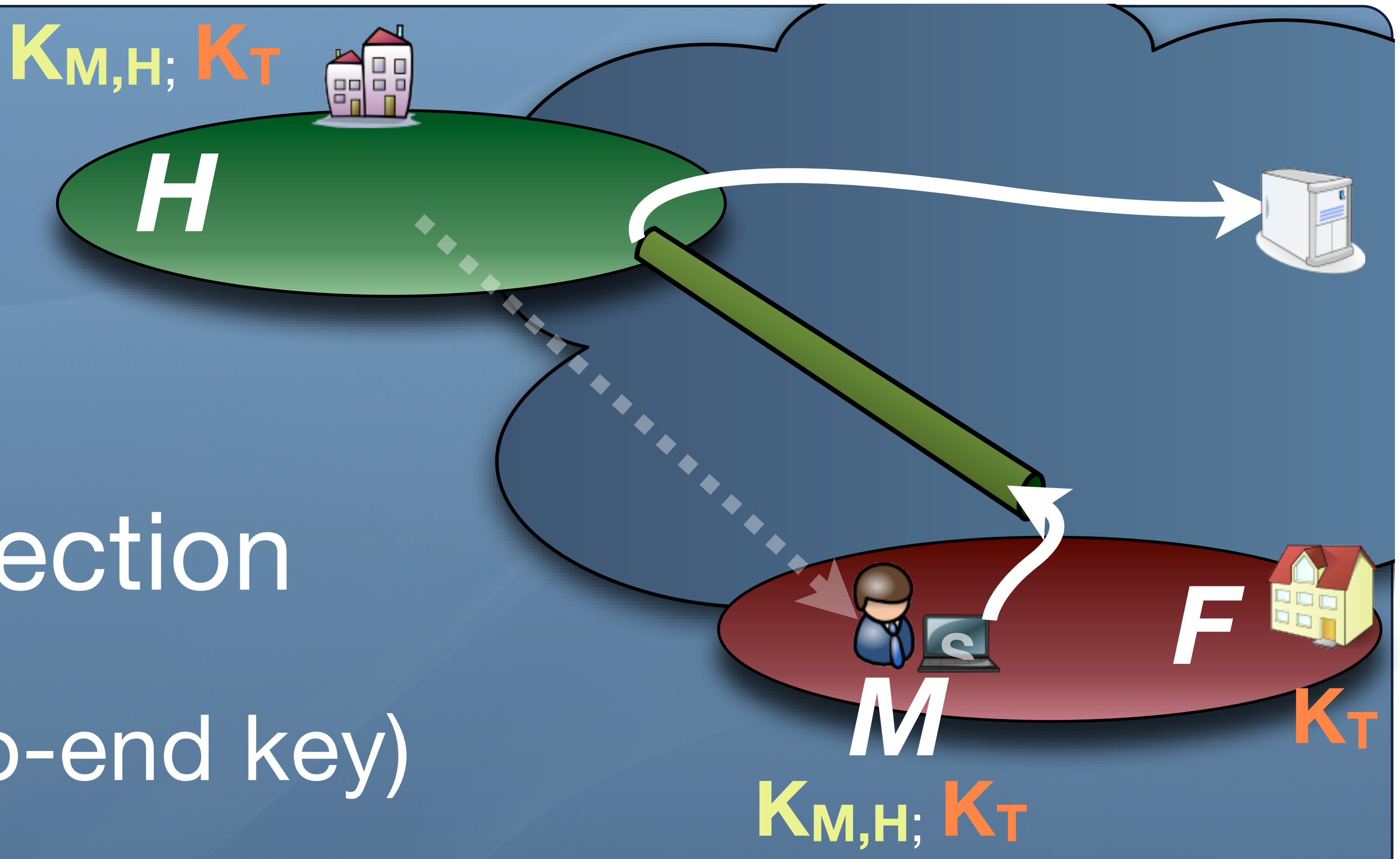
$\mu_M,\sigma_F(*)$

$K_T =PRF_{kt}(1,sid)$

$K_{M,H} = PRF_{kM}(2,sid)$

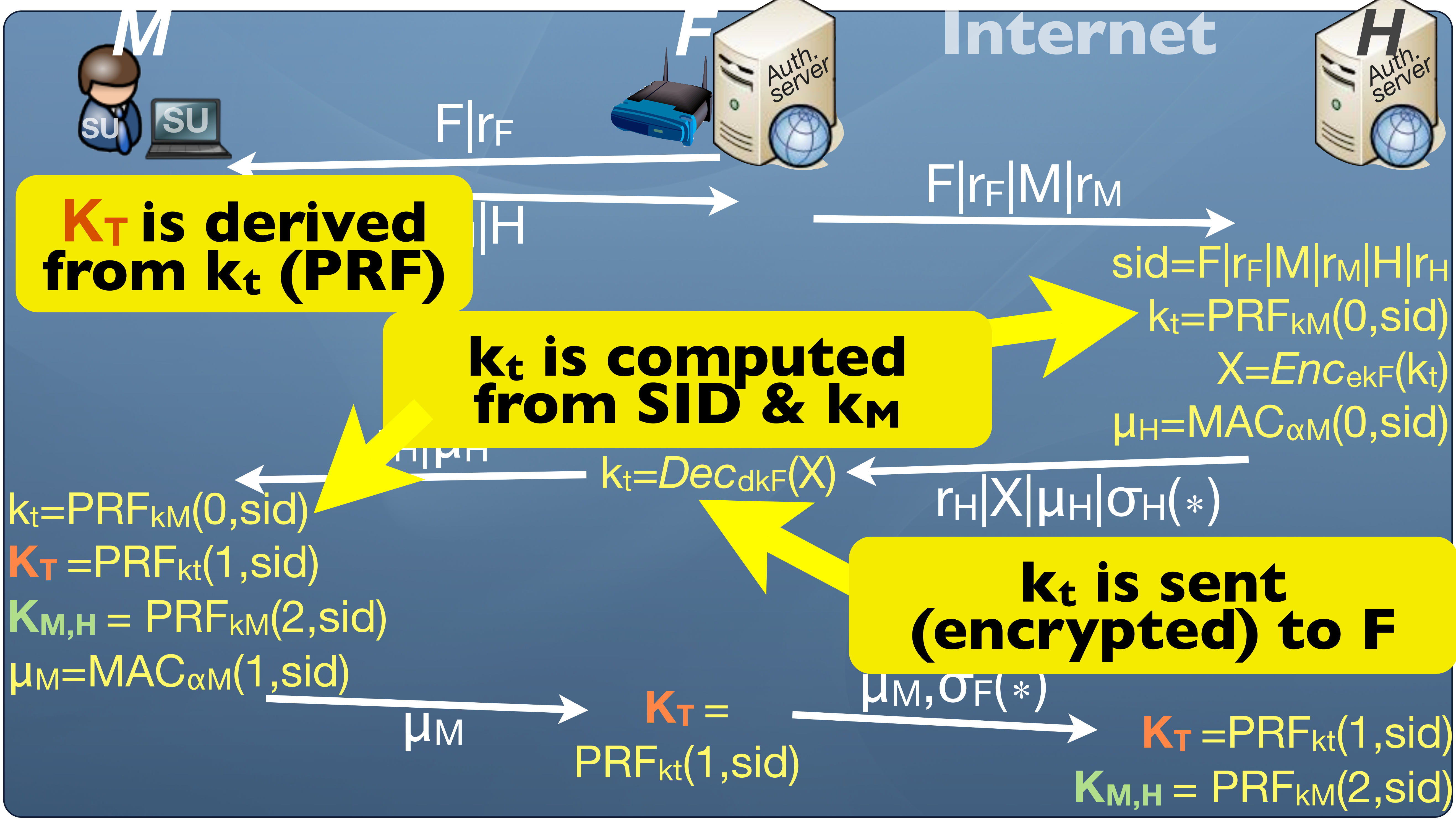
Security Goals

Key establishment



- End-to-end protection
  - ➡ $K_{M,H}$ (end-to-end key)
- Protection of communication between M, H and F
  - ➡ K_T (tunnel key)

AWRT - The protocol (simplified)



$F|r_F$

$|H$

$F|r_F|M|r_M$

$sid=F|r_F|M|r_M|H|r_H$
$k_t=PRF_{k_M}(0,sid)$
$X=Enc_{ek_F}(k_t)$
$\mu_H=MAC_{\alpha_M}(0,sid)$

$r_H|X|\mu_H|\sigma_H(*)$

$k_t=Dec_{dk_F}(X)$

$H|\mu_H$

$k_t=PRF_{k_M}(0,sid)$
$K_T=PRF_{k_t}(1,sid)$
$K_{M,H} = PRF_{k_M}(2,sid)$
$\mu_M=MAC_{\alpha_M}(1,sid)$

μ_M

$K_T =$ $PRF_{k_t}(1,sid)$

$\mu_M,\sigma_F(*)$

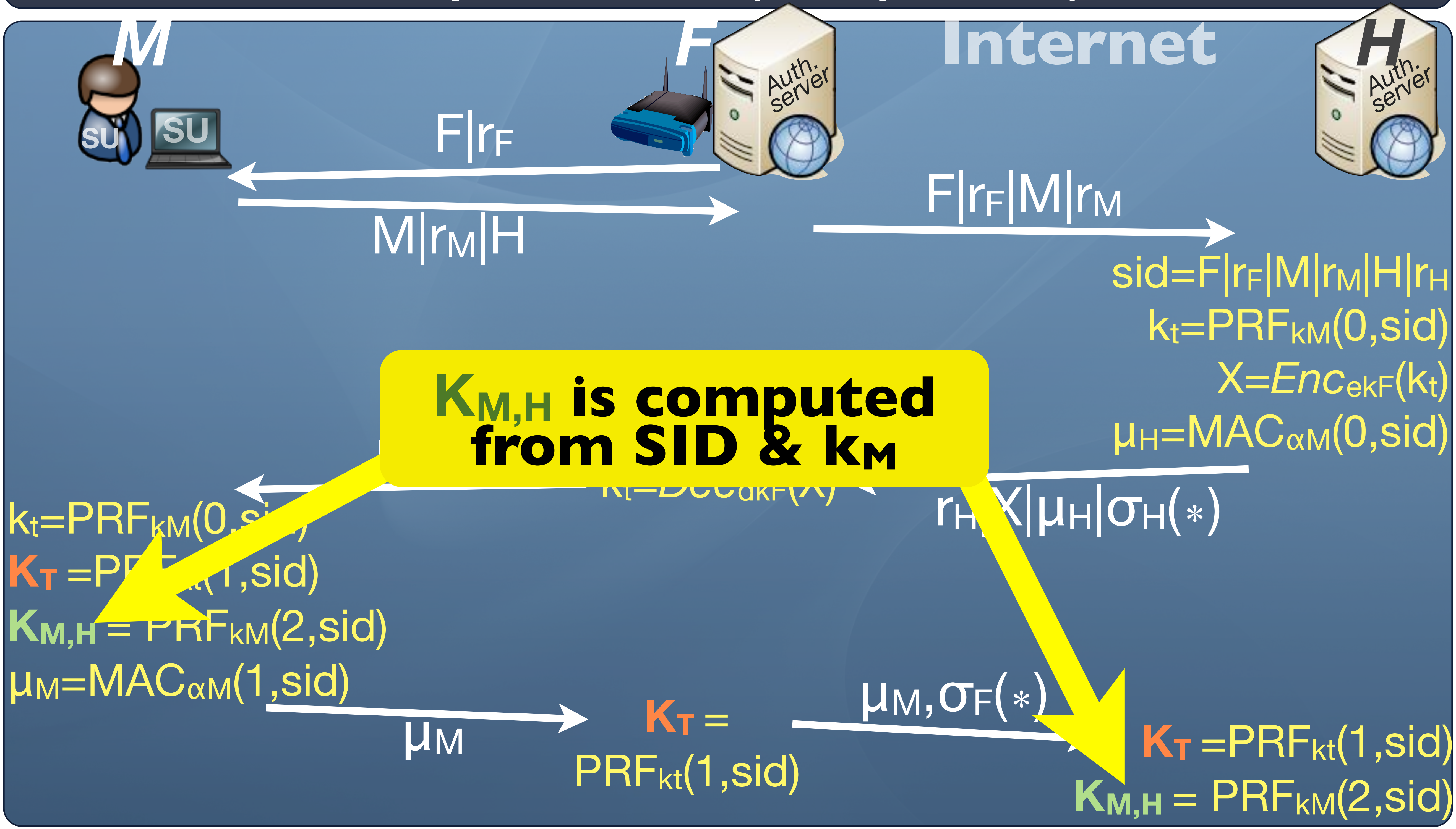
$K_T=PRF_{k_t}(1,sid)$
$K_{M,H} = PRF_{k_M}(2,sid)$

K_T is derived from k_t (PRF)

k_t is computed from SID & k_M

k_t is sent (encrypted) to F

AWRT - The protocol (simplified)



$F|r_F$

$M|r_M|H$

$F|r_F|M|r_M$

$sid=F|r_F|M|r_M|H|r_H$
$k_t=PRF_{kM}(0,sid)$
$X=Enc_{ekF}(k_t)$
$\mu_H=MAC_{\alpha M}(0,sid)$

$r_H|X|\mu_H|\sigma_H(*)$

$k_t=Dec_{dkF}(X)$

$K_{M,H}$ is computed from SID & k_M

$k_t=PRF_{kM}(0,sid)$
$K_T=PRF_{kt}(1,sid)$
$K_{M,H}=PRF_{kM}(2,sid)$
$\mu_M=MAC_{\alpha M}(1,sid)$

μ_M

$K_T=PRF_{kt}(1,sid)$

$\mu_M,\sigma_F(*)$

$K_T=PRF_{kt}(1,sid)$
$K_{M,H}=PRF_{kM}(2,sid)$

Remarks on efficiency

- The number of messages exchanged between F and H is the key point for protocol duration
  - The mobile can already send data packet after one RTT
- M can be a light mobile device (e.g., a smart phone)
  - No asymmetric key crypto computation in M

Practical Realizations of the Mechanism

Proposals

- AWRT :
  - In IEEE802.1X as a new EAP method
- The tunnel between F and H
  - A Layer-2 tunnel
- End-to-End security
  - ESP (Encapsultating Security Payload) (within IPsec)

Optional Protocol Extensions

(discussed in the paper)

- Forward Secrecy
  - Using DH techniques
- Denial-of-Service and Hijacking protection
- Confidentiality for M
- Accounting for Roaming

Conclusion

Summary of security advantages

- Tunnels permits :
  - For F: No harm to its network and reputation
  - For M: have the same services as “at home”
- Force M to use the tunnel (and to H !)
- F is authenticated by H ! (not by M that can be subjected to phishing/spoofing)

Conclusion

Contributions

- WRT is not really "new" but it is the first time it is used for a such use
- AWRT permits 3-party-authentication & -key agreement in WRT
  - Based on a formal security model
  - A protocol has been designed

Questions ?

Mark Manulis
mark@manulis.eu

UCL Crypto Group
(former member)
www.dice.ucl.ac.be/crypto/

Damien Leroy
damien.leroy@uclouvain.be

IP Networking Lab

http://inl.info.ucl.ac.be