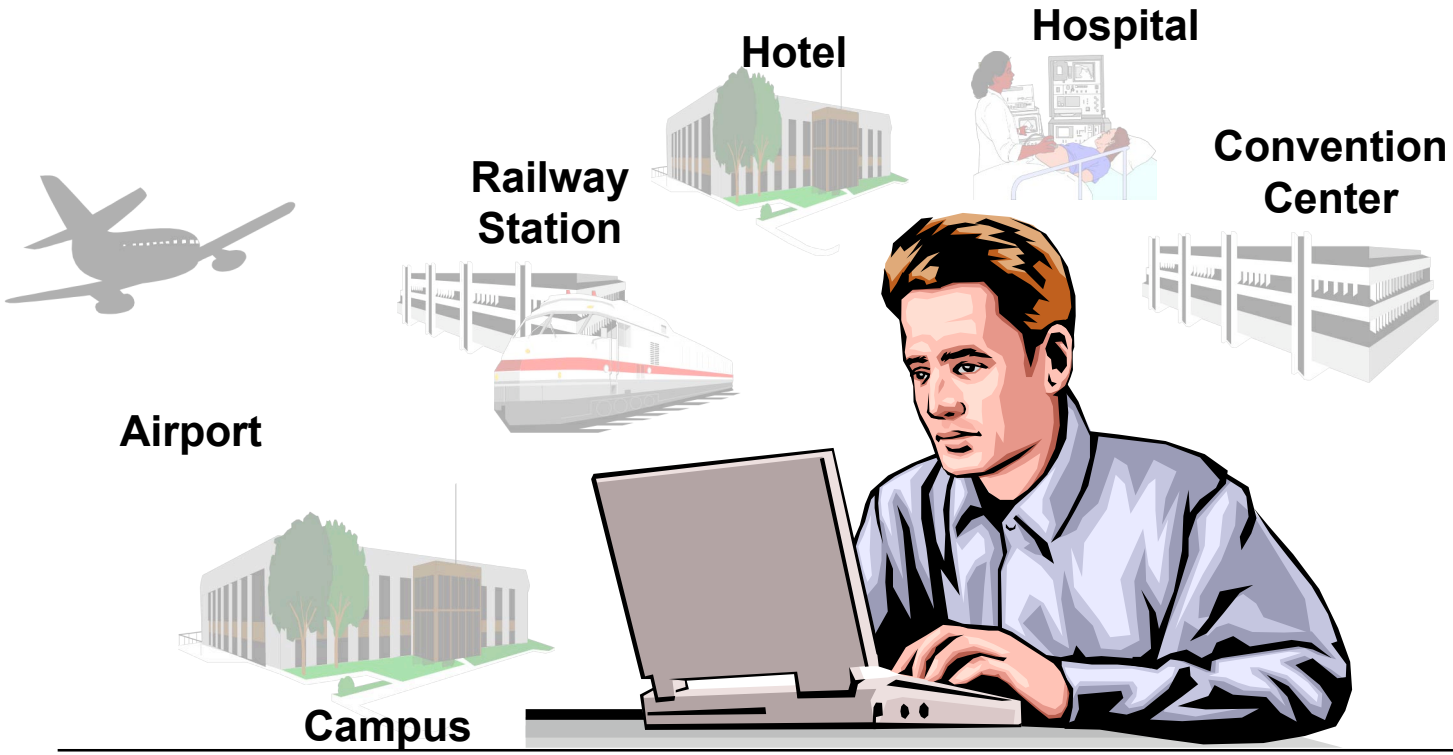
Selling network access

Views from a business perspective

Max Riegel
Siemens

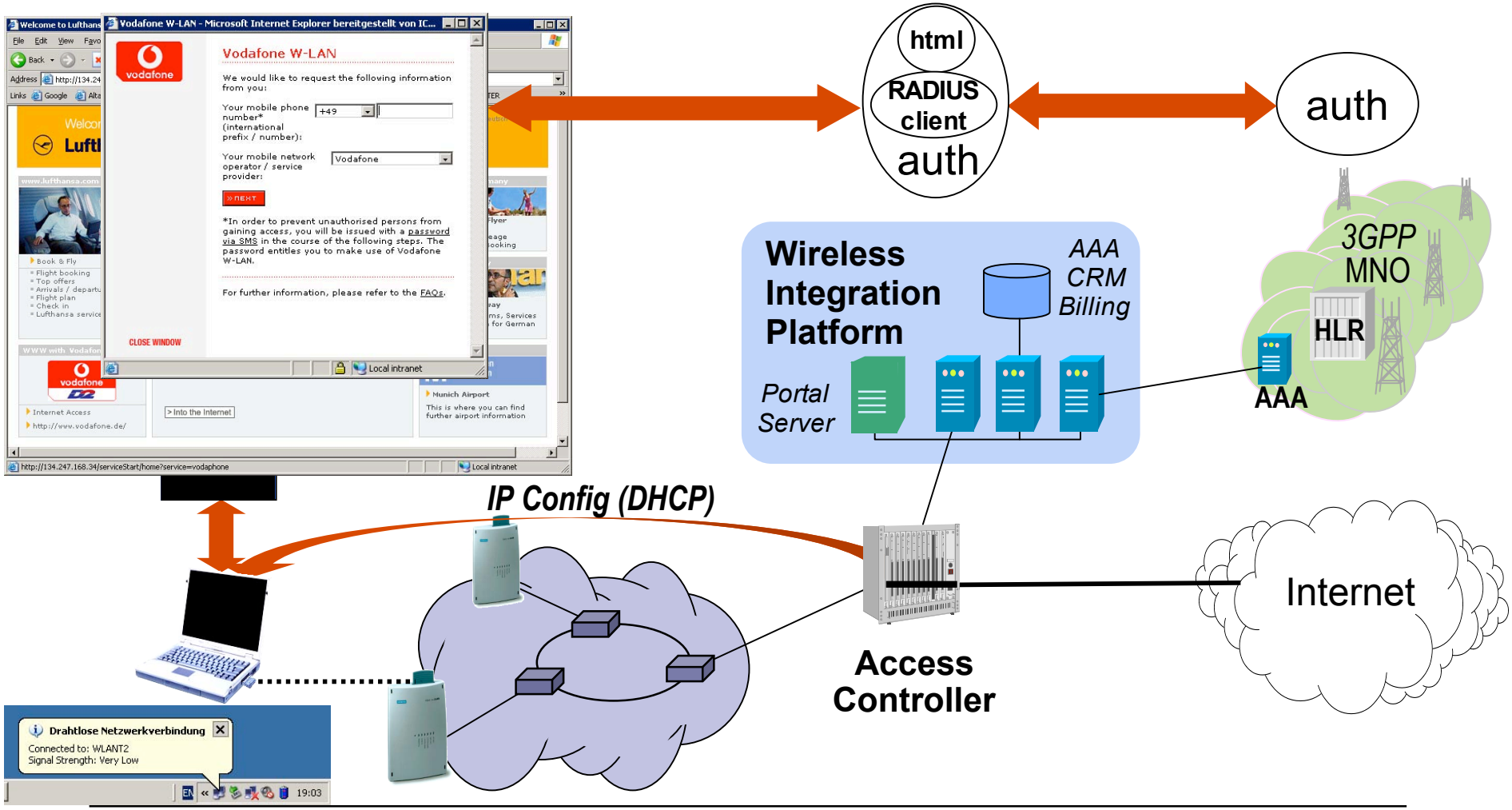
Serving WLAN customers in public hot spots...

... often means selling network access in a competitive environment.



Portal based access control

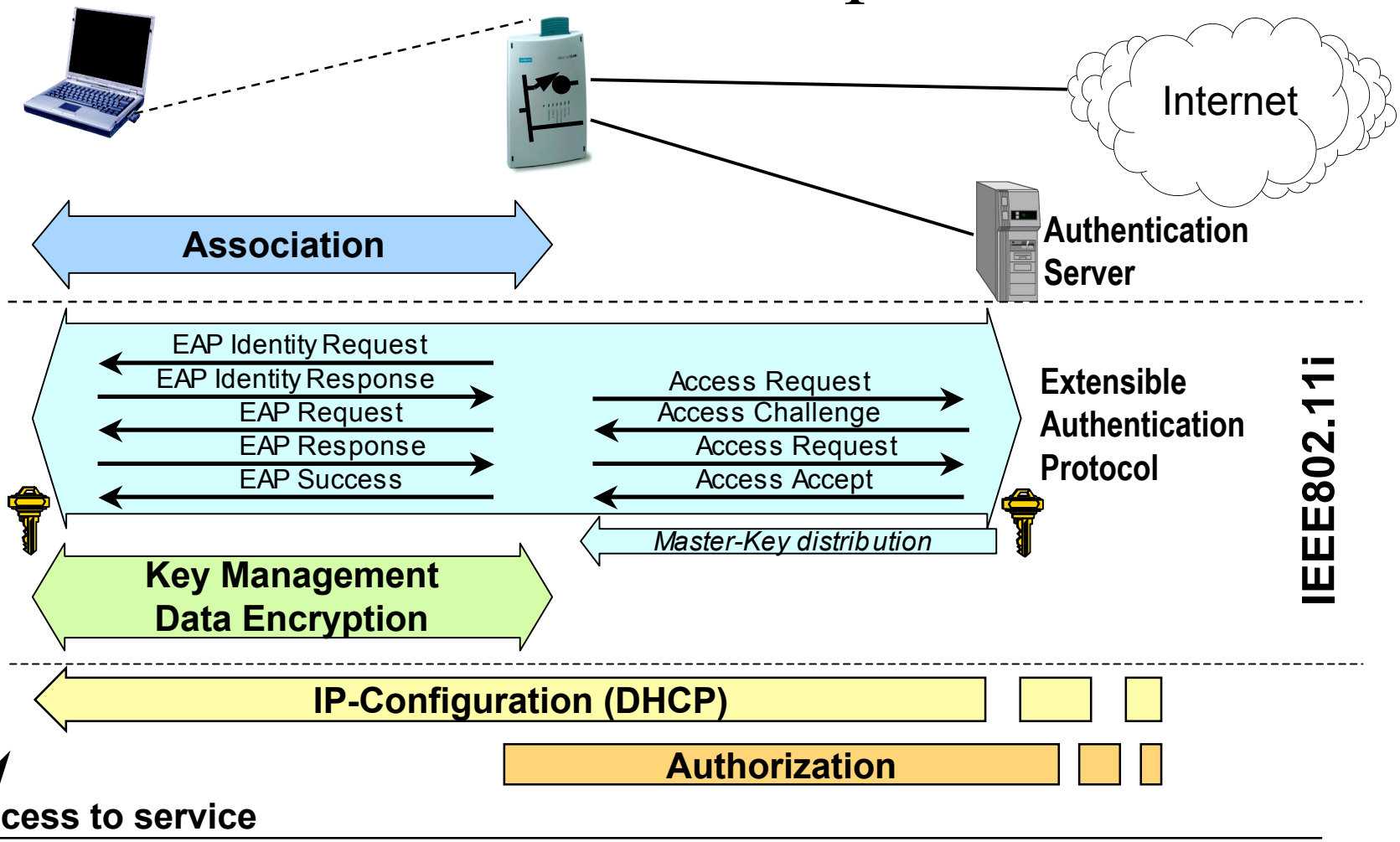
also known as UAM



Portal based access control – not everybody's darling!

- Portal based access control for public WLAN has been specified within the WiFi Alliance WISPr 1.0 Recommendation
  - Establish a common look-and-feel of the portal based access control.
- Portal based access control is currently used by all commercial public hotspots
- People in standardization deprecate the usage of UAM due to
  - No 2G/3G-like automatic network association
  - SIM support complicated
  - WLAN link unsecured
    - weak mutual authentication, no over-the-air encryption, session hijacking
  - Browser redirect does not always work
- IEEE802.1X/EAP (Extensible Authentication Protocol) is seen as the best solution for public access.
  - has been adopted by IEEE802.11i

IEEE802.11i adds EAP and data encryption into the WLAN access procedure



Public WLAN access with 802.11i/EAP fixes the bugs but creates new issues

- 802.11i/EAP solves the issues for
  - 2G/3G-like automatic network association w/ SIM
  - Secured WLAN connection

... but creates new issues:

- Network Discovery and Selection Problem
  - details see: draft-ietf-eap-netsel-problem-00.txt
  - Access network discovery, identifier selection, AAA routing, payload routing; or: Discovery, Decision, and Selection
- User interaction and help in the case something goes wrong
- Support for more sophisticated business models, e.g.
  - Selection of different services during a particular session
  - Anonymous services, e.g. enrollment support

... issues which are well supported by the UAM!

Two approaches for selling (access)

802.11i/EAP is like a *'Vending machine'*

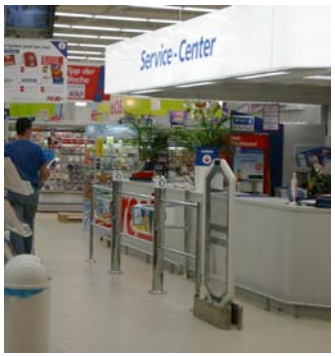
- Put in the right coin, push the button and you are done.

- If something fails, you are lost.
- 'Dont ask

Portal based access control is like a *'Mall'*

- Open anonymous access

- Very attractive and flexible to the customer

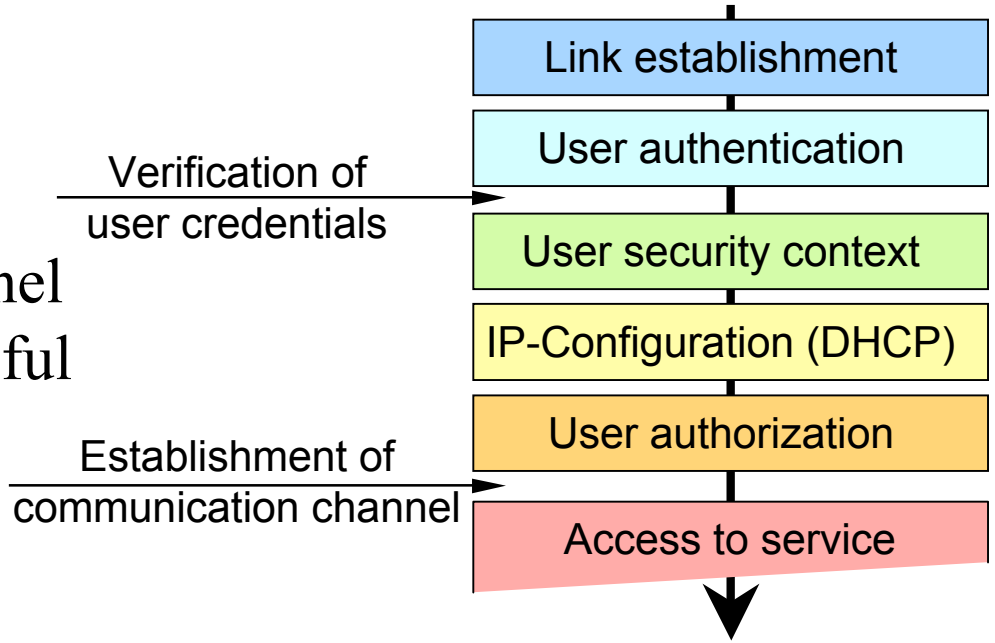


- 'Have fun, but it may take time'

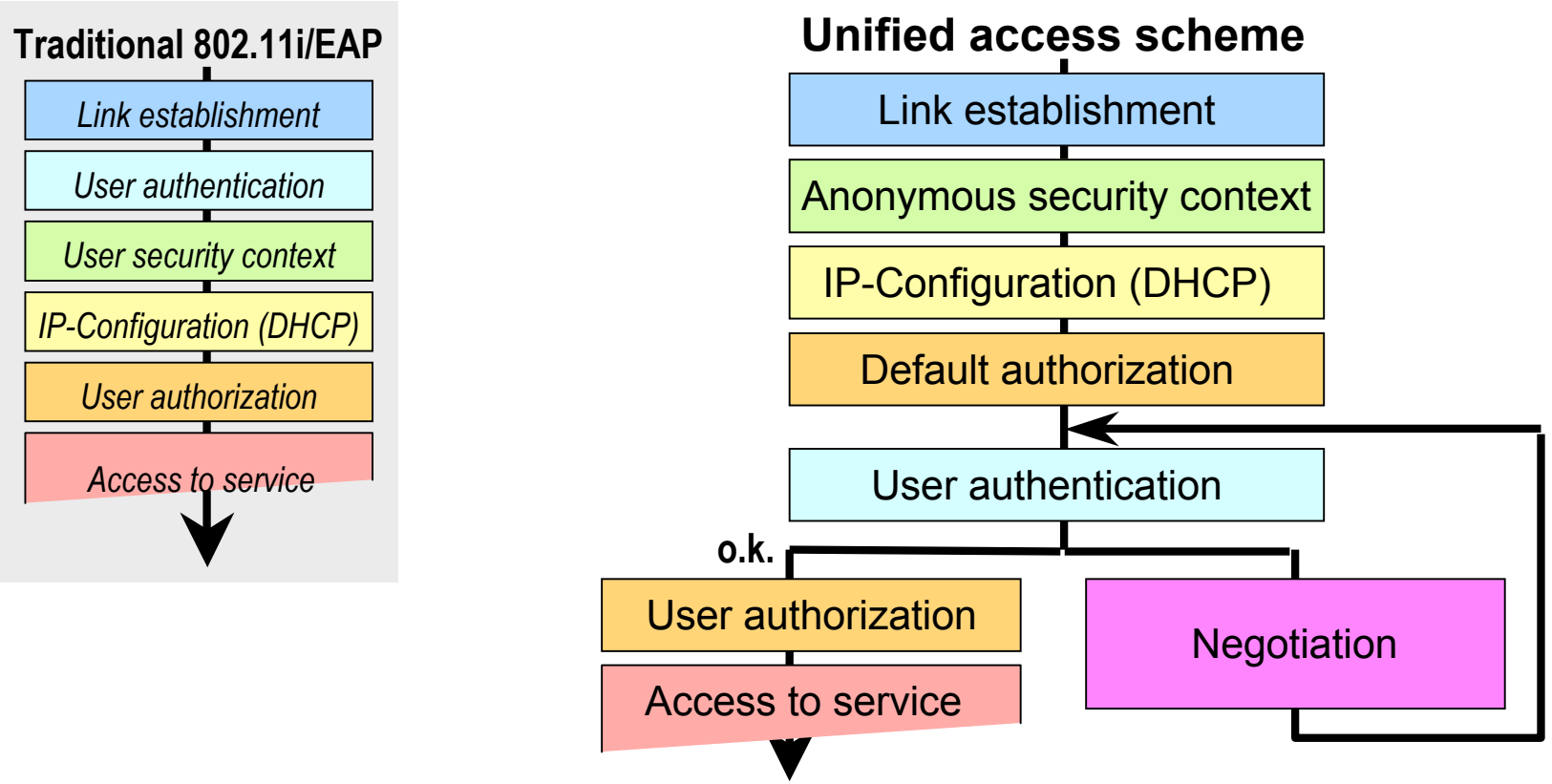
Combining EAP and UAM

- Both 802.11i/EAP as well as UAM are valuable approaches
  - 802.11i/EAP for the experienced, repeating user
  - UAM for the 'beginner' and for exception cases
- Combining EAP & UAM is currently not possible.
  Why?

  No communication channel available prior to successful user authentication.



An unified approach for network access control



Conclusion

- UAM as well as EAP are valuable solutions for access control.
- ‘Secured’ UAM is currently not possible.
- An anonymous secured media-rich communication channel is needed before user authentication and authorization.
- There are several potential solutions for postponed authentication:
  - Enhanced EAP methods
  - Smart client based on https (see WISPr)
  - Layer-3 authentication protocol (PANA)
- Most urgent for public WLAN access,
  but may lead to a general solution later.
- Should become a topic in IEEE802.11 WIEN