Wi-Fi is everywhere!

Wi-Fi Protected Access

Media Briefing

Agenda

- Opening remarks
- Introducing WPA
- Securing Wi-Fi Today
- WPA Key Messages
- Timelines & Roadmaps
- WPA in the Enterprise
- WPA in the Home & Small Office
- Summary
- Detailed technical briefing material

Introducing WPA

- Wi-Fi Protected Access (WPA) is a proactive response by the industry to offer an immediate and strong security solution
- WPA
  - Standards-based, interoperable security specification
  - Significantly increases the level of data protection and access control for existing and future wireless LAN systems
- WPA is a subset of the 802.11i draft standard and will maintain forward compatibility

Securing Wi-Fi Today

- There are technologies that can be used to secure your Wi-Fi LAN today
  - Virtual Private Networks (VPNs)
  - 802.1X based authentication with WEP encryption (dynamic WEP)
  - WEP is still a good deterrent for “casual” snoopers
- Wi-Fi Protected Access will replace WEP as standard Wi-Fi security

WPA Key Messages

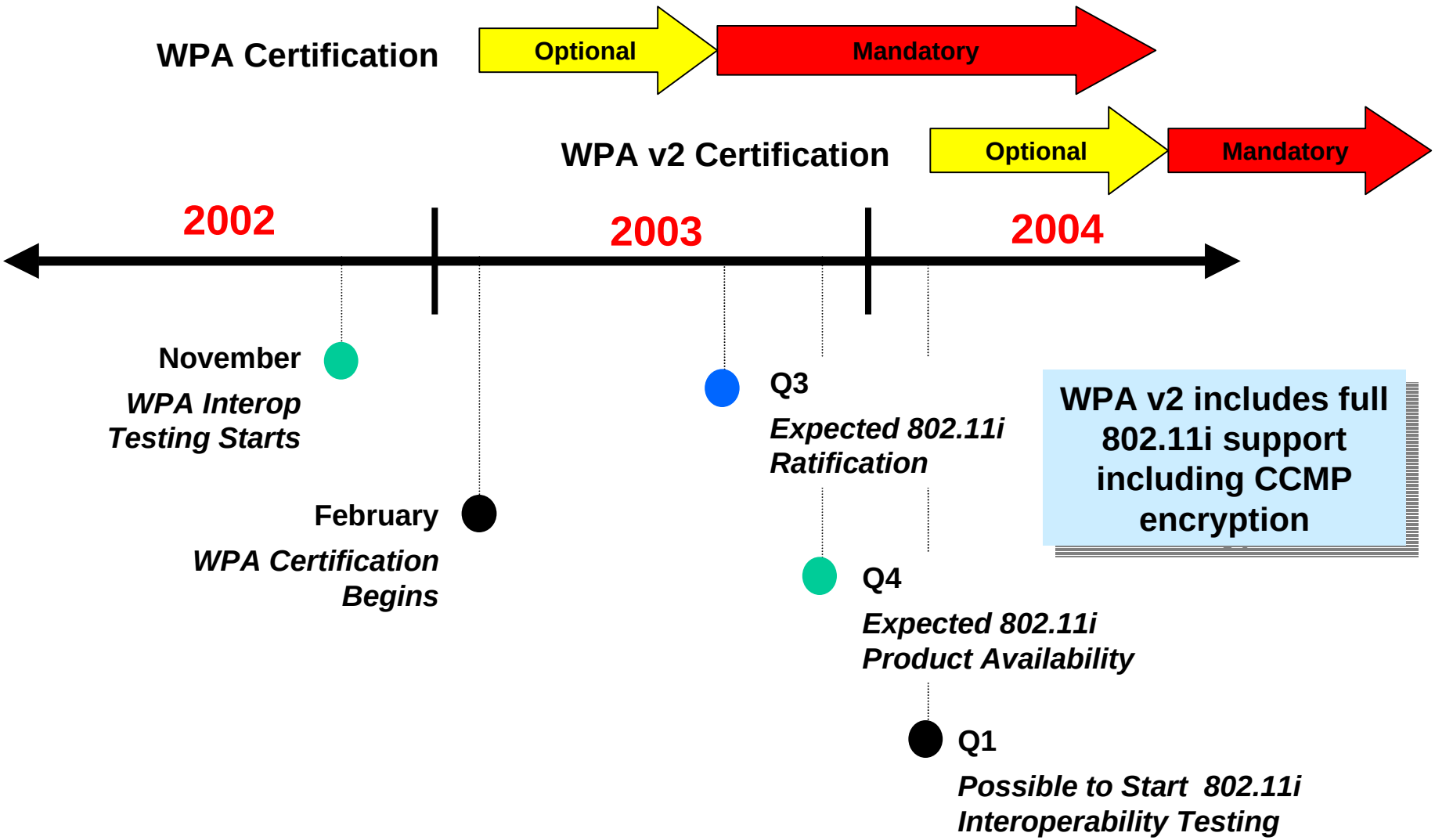
- Customers needed a solution now!
- TGi will be available in about a year
- Both backward and forward compatibility
- Will cover the majority of products on the market today
- Great solution for business
- Great solution for the home – Preshared key
- Let’s look at when it will be available…

WPA Interoperability Testing Timeline

Tasks \ Weeks	Nov 8		Nov 22	Nov 29	Dec 6	Dec 13		Jan 3	Jan 10	Jan 17	Jan 24	Jan 31
Draft Test Plan Completed	◇											
Interop testing (test bed devt.)			◇			◇		◇			◇	
Certification starts (Feb 3)											**Feb 3** ★	

- Some early interoperability testing has already started
- Formal certification is expected to start in Q1 of 2003

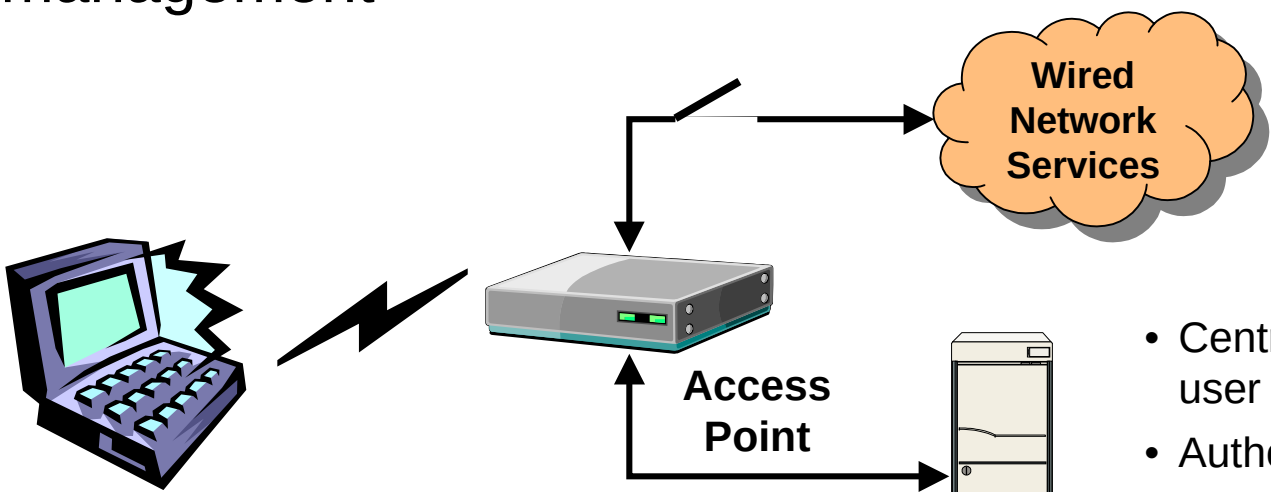
Wi-Fi Alliance Security Roadmap



WPA in the Enterprise

- In the enterprise, WPA is used in conjunction with an authentication server to provide centralized access control and management

Access to wired and wireless network services is allowed only after successful user authentication and encryption key distribution



User credentials can include:

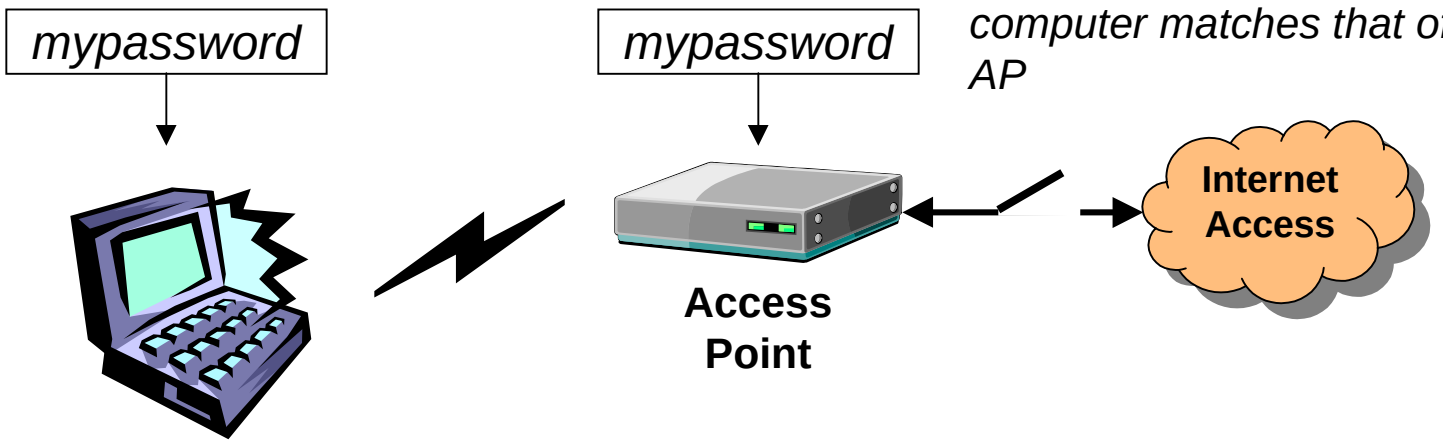
- Username & password
- Certificates
- Other

- Centralized management of user credentials
- Authorization of users requesting network access
- Generation of session and group encryption keys

WPA in the Home & Small Office

- In the home or small office, WPA can be used in a *pre-shared key* mode which does not require an authentication server

Access to the internet and rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the AP



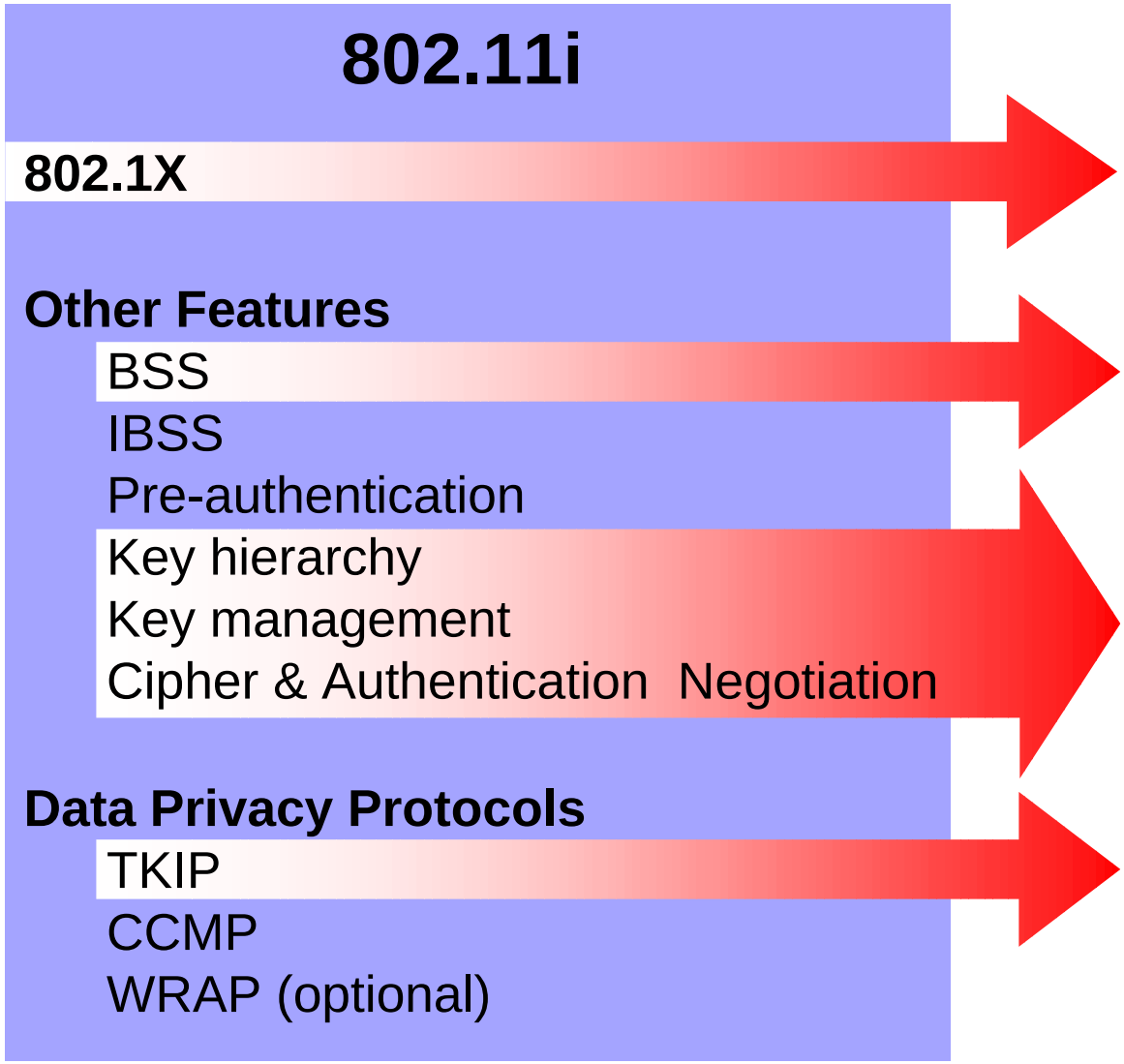
Summary

- Secure your Wi-Fi LAN!
  - VPNs, 802.1X, and other technologies can be used today
  - In the near future you will be able to use WPA
- When properly installed, Wi-Fi Protected Access will provide
  - Strong over-the-air data protection
  - Strong network access control
- The Wi-Fi Alliance expects formal certification of WPA to begin in first quarter of 2003
- Look for WPA software upgrades to start to appear in the next several months

Wi-Fi Legacy Security

- Wired Equivalent Privacy (WEP) defined in 1999, 802.11 standard
  - Intended to provide a level of protection equivalent to a wired system which can rely on physical protection
  - Provides link layer encryption only
- The standard also defines shared key authentication for user authentication
- Wired Equivalent Privacy (WEP) has been shown to have several vulnerabilities
- Native 802.11 authentication mechanisms are easily overcome

WPA is a snapshot of 802.11i



Wi-Fi Protected Access

- Implement what is stable and bring it to market
- Continue work on 802.11i