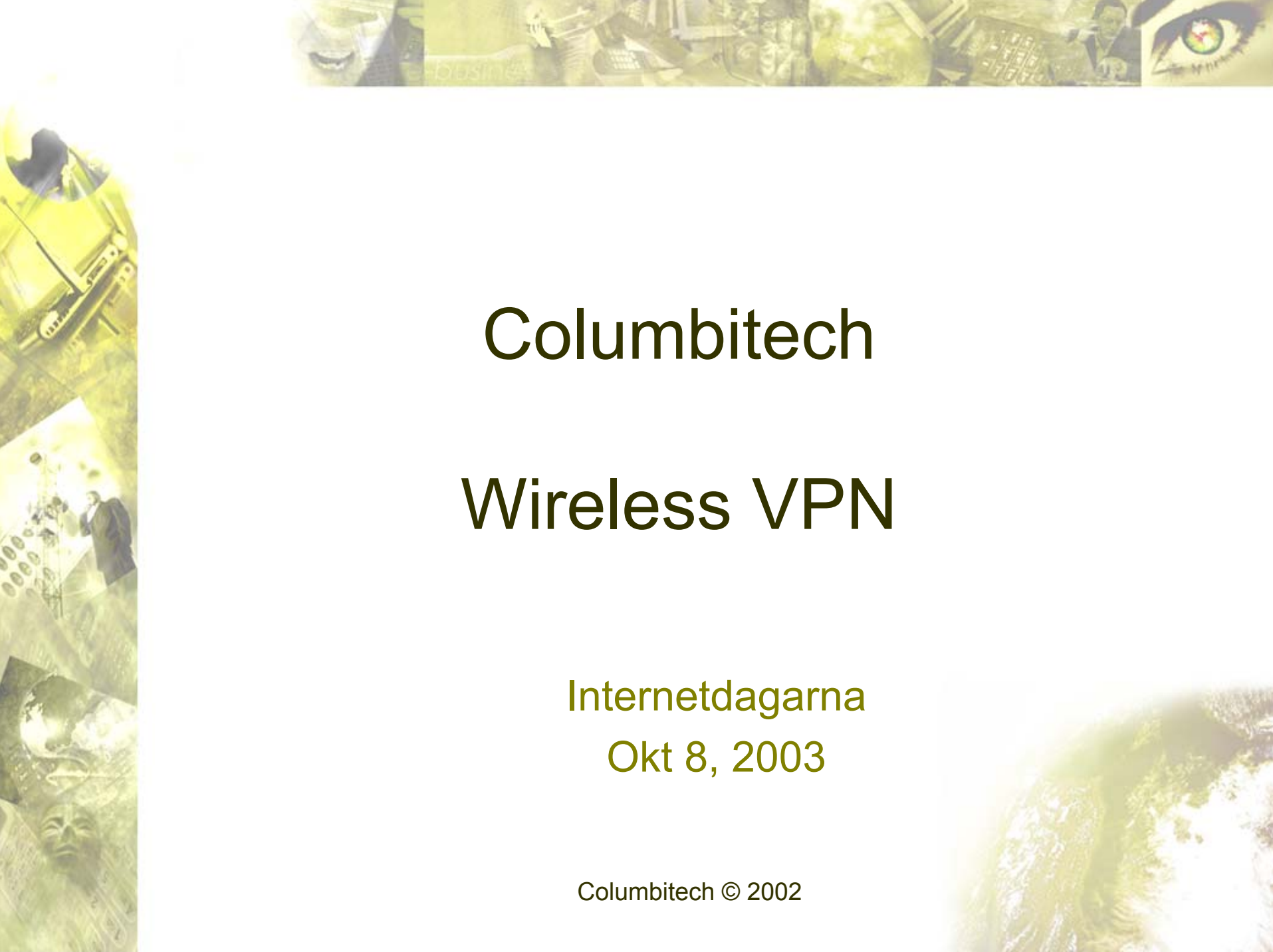




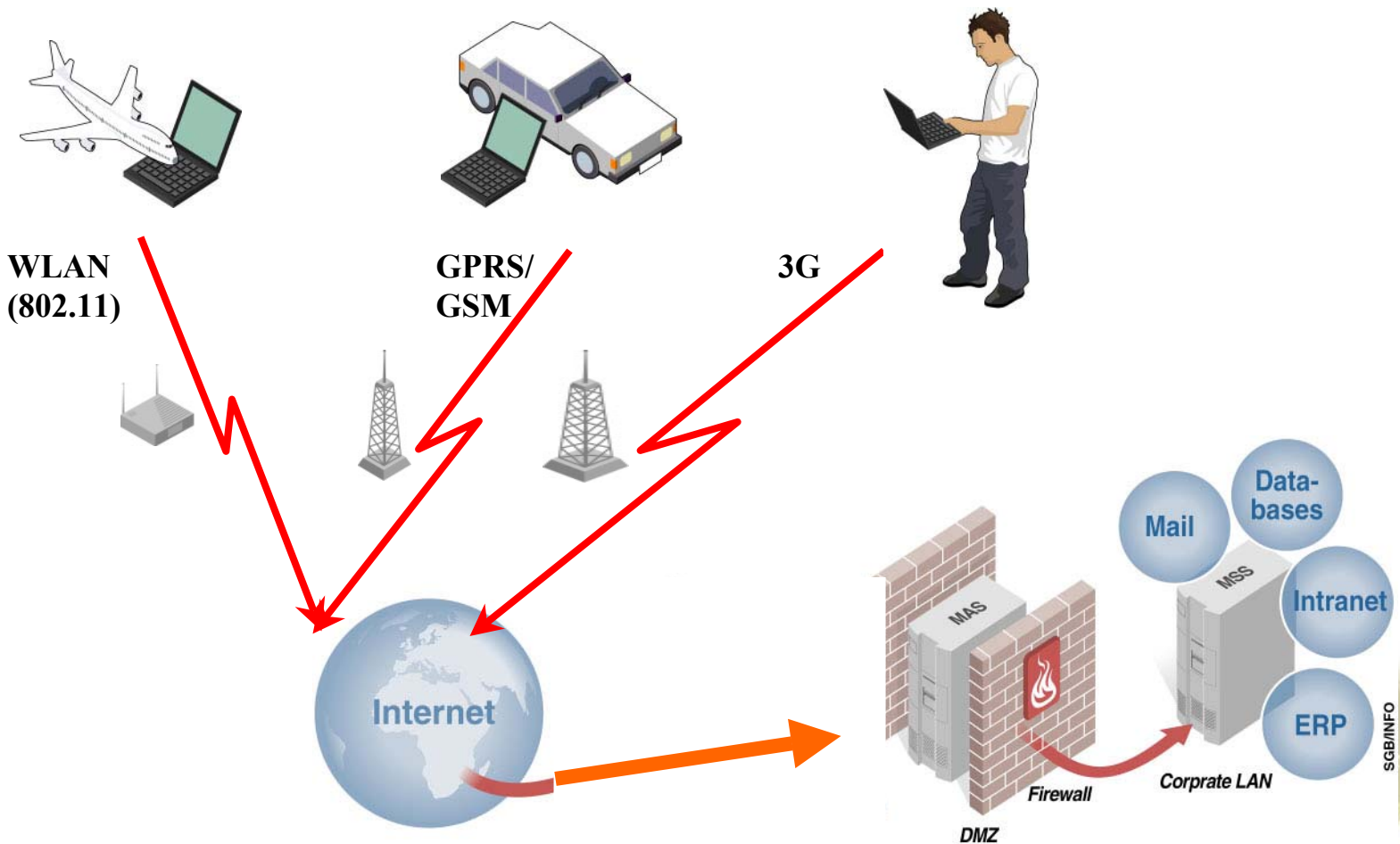
Columbitech

Wireless VPN

Internetdagarna
Okt 8, 2003

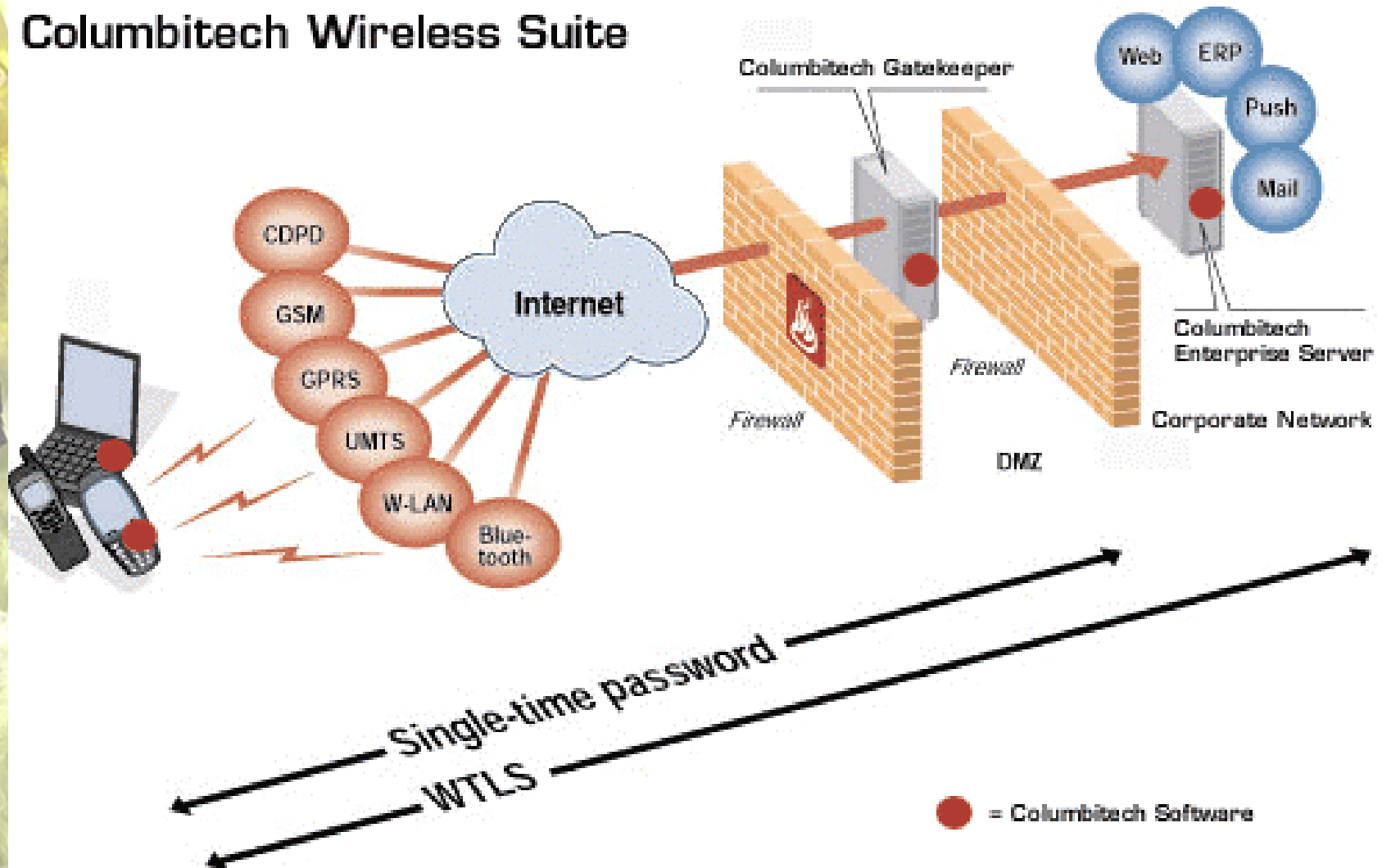
Columbitech © 2002

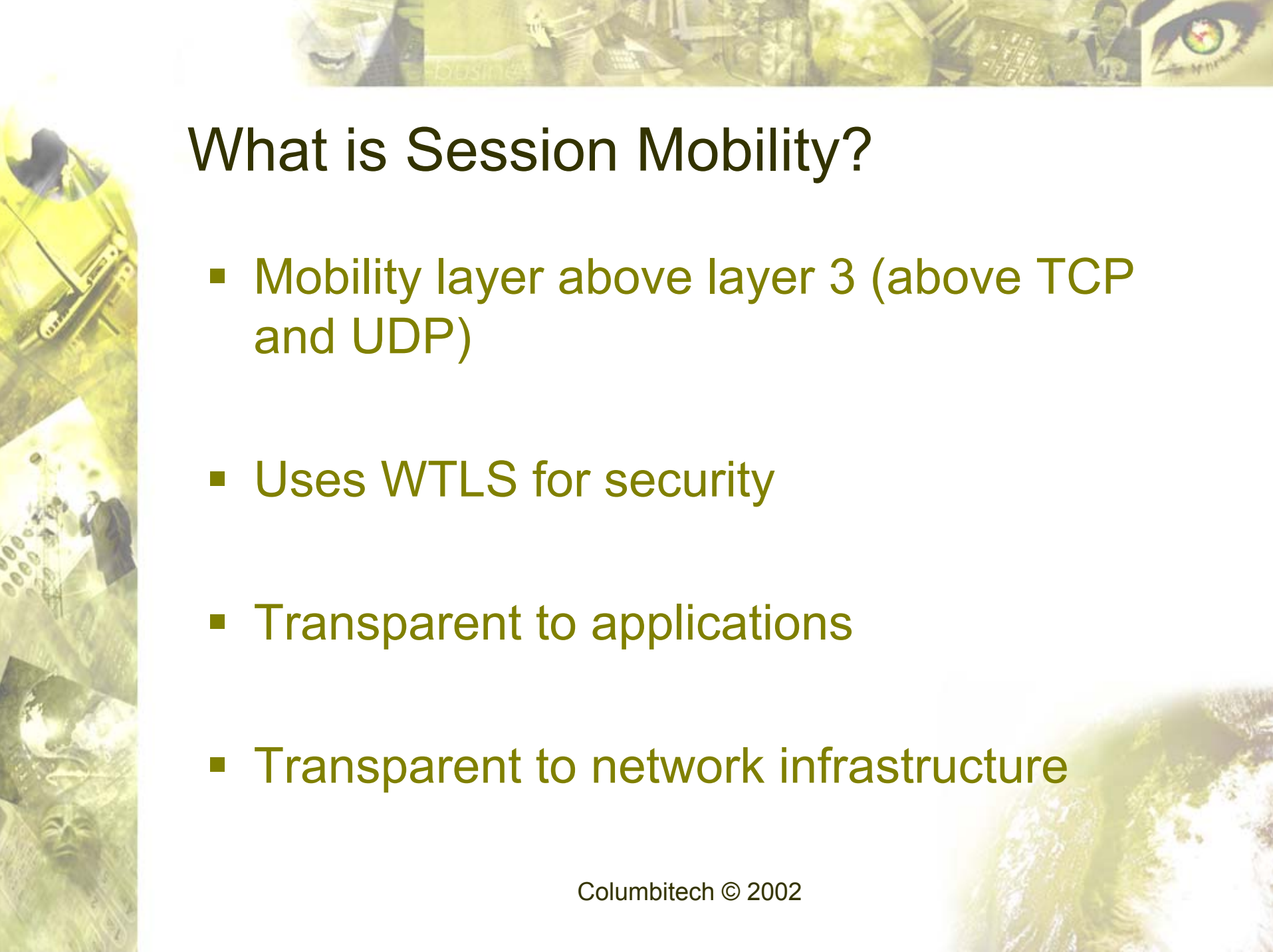
Key value added: Seamless network handover



Columbitech architecture

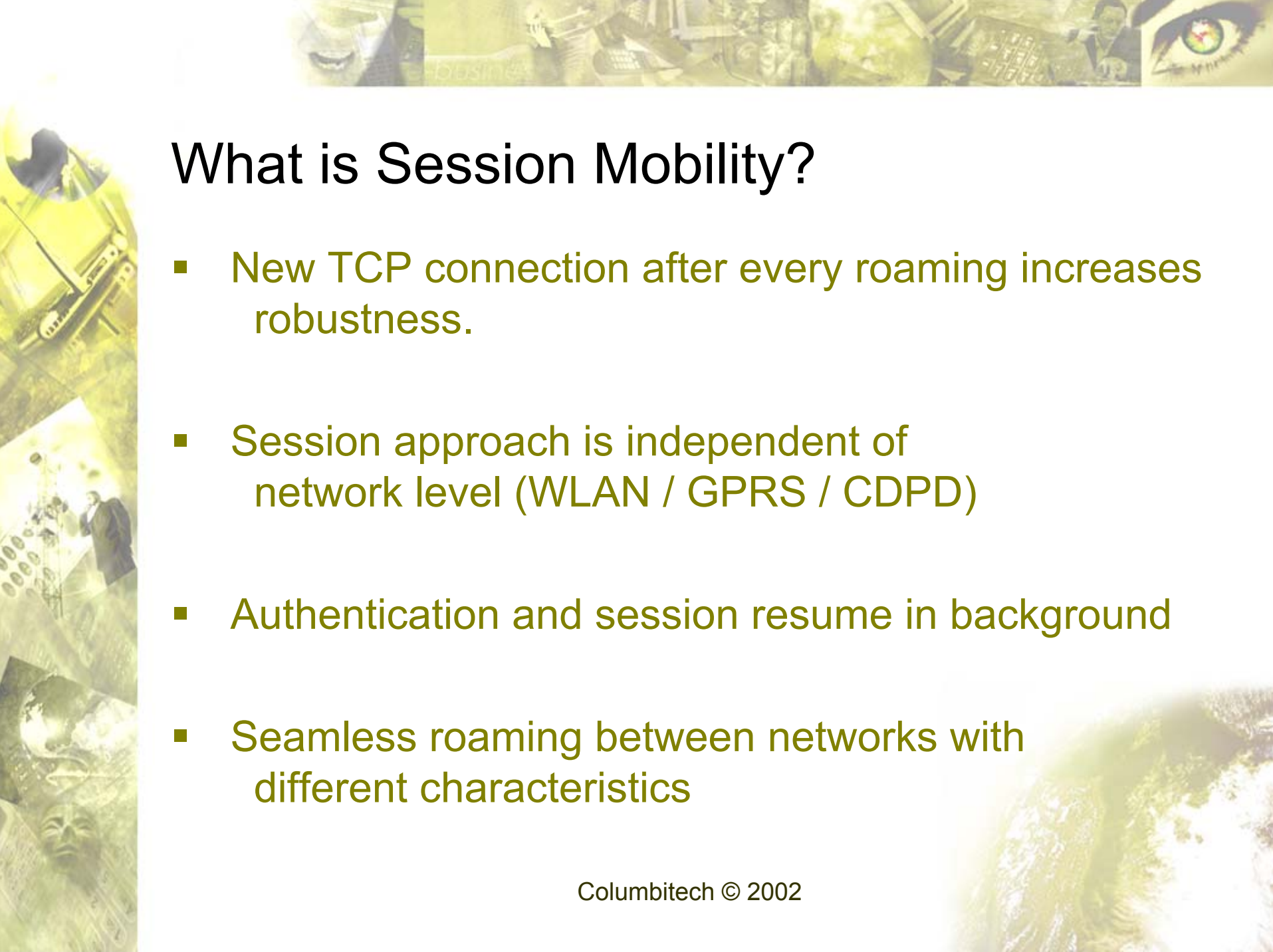
Columbitech Wireless Suite





What is Session Mobility?

- Mobility layer above layer 3 (above TCP and UDP)
- Uses WTLS for security
- Transparent to applications
- Transparent to network infrastructure



What is Session Mobility?

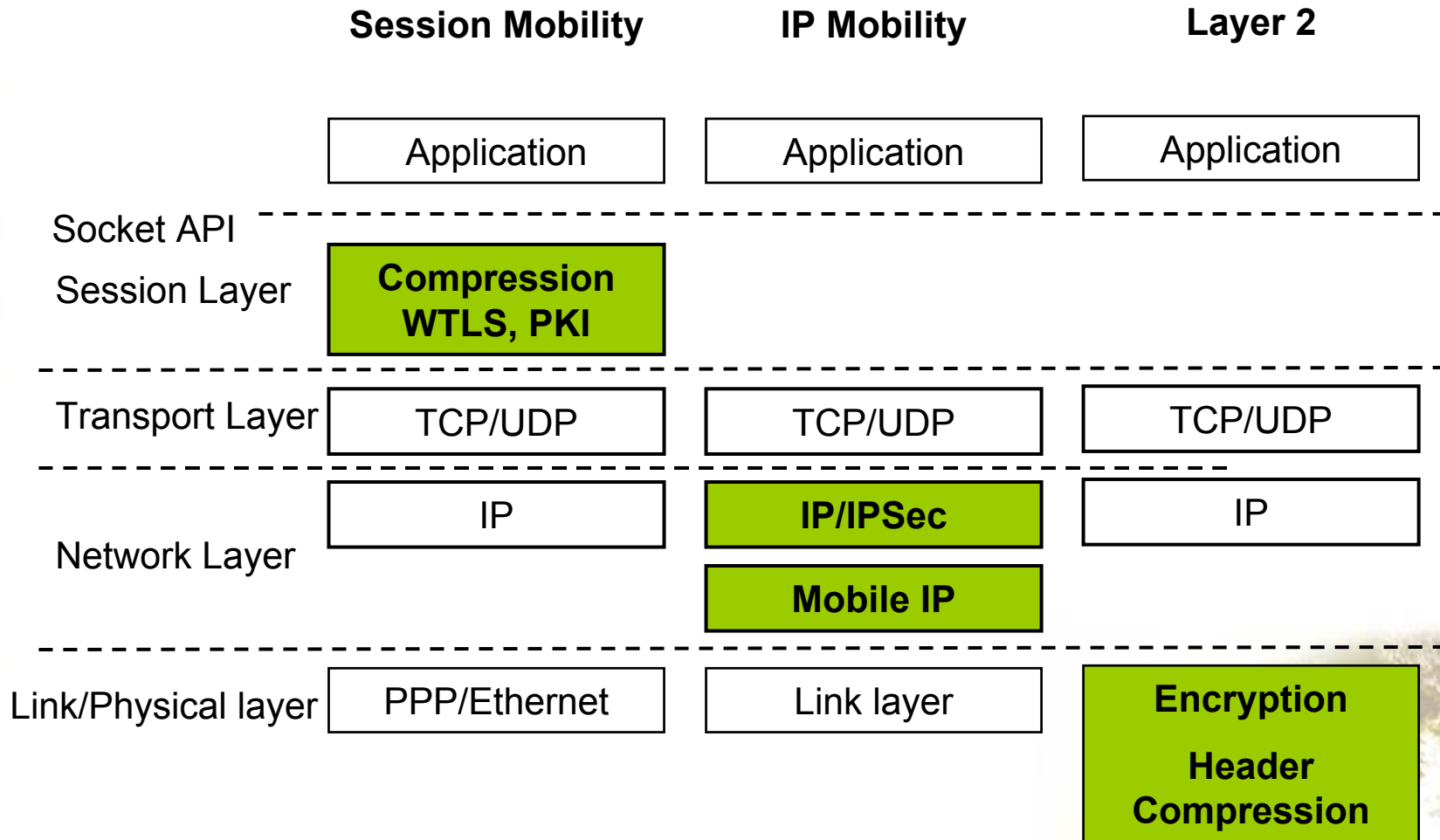
- New TCP connection after every roaming increases robustness.
- Session approach is independent of network level (WLAN / GPRS / CDPD)
- Authentication and session resume in background
- Seamless roaming between networks with different characteristics



Why Session Mobility

- ❑ Solves NAT server problems
 - WTLS does not encrypt transport protocol headers
- ❑ Solves Transport layer problems
 - Implemented above transport layer
 - protects applications from connection failures
- ❑ More efficient compression/optimisations
 - Session level approach means compression is performed on large data streams
- ❑ Session resume
 - WTLS session is automatically resumed after network failures - user remains logged in

Communication stack

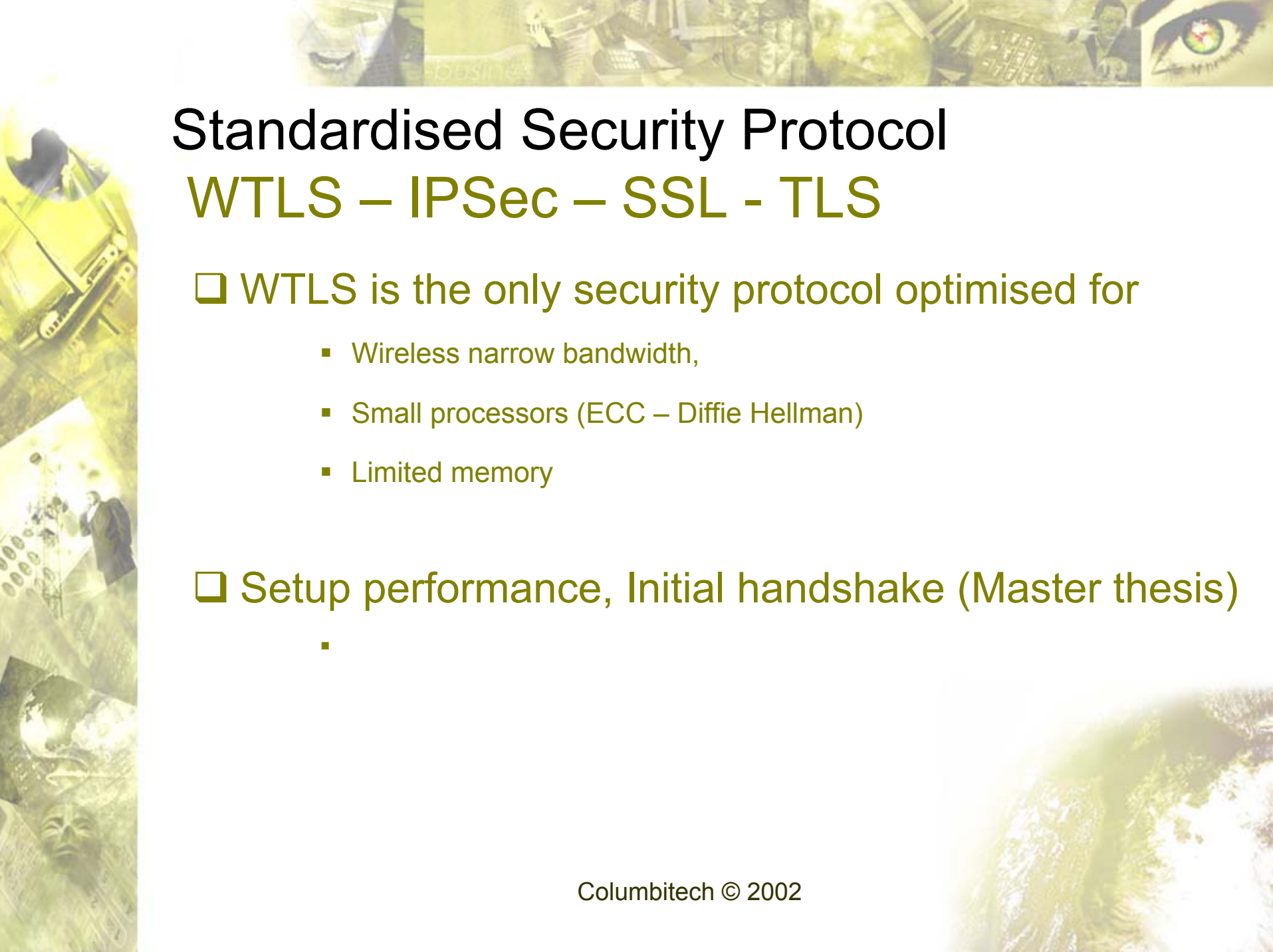


What do we mean by security?

- **Confidentiality** **Hiding of information**
- **Authentication** **Proof of identity**
- **Integrity** **Proof that information is unaltered**
- **Non-repudiation** **Denial is made impossible**
- **Authorization** **What an entity is allowed to do**

Key issues in wireless security

- End-to-end security
- Paradox to combine strong security and convenience
- Slower processors
- Limited memory
- VPN access over Public Network both wireless and wired.



Standardised Security Protocol

WTLS – IPSec – SSL - TLS

- ❑ WTLS is the only security protocol optimised for
 - Wireless narrow bandwidth,
 - Small processors (ECC – Diffie Hellman)
 - Limited memory
- ❑ Setup performance, Initial handshake (Master thesis)
 -