Bluetooth Security Architecture

Version 1.0

This White Paper describes a flexible security architecture for Bluetooth that allows different security levels for applications. While Bluetooth provides link-level authentication and encryption, enforcing at only this level prevents user-friendly access to more public-oriented usage models such as discovering services and exchanging business cards. This architecture uses the link-level security mechanisms of Bluetooth to enforce the service level security policy (security mode 2) of the Generic Access Profile.

Special Interest Group (SIG)

The following companies are represented in the Bluetooth Special Interest Group:
Ericsson Mobile Communications AB
IBM Corp.
Intel Corp.
Nokia Mobile Phones
Toshiba Corp.

Revision History

Revision	Date	Comments
0.0	1999-03-29	first draft, based on discussion at the SW face-to-face meeting in chandler, AZ
0.0.1	1999-03-30	Requirement on limited user intervention added 2 requirements in question added Start work on procedures (general behavior, Handling of RFCOMM)
0.0.2	1999-04-01	Incorporated feedback from Paul and Chatschik
0.0.3	1999-04-07	Feedback from Brian Redding
0.1	1999-04-09	Integrate decisions from the meeting 1999-04-08 Add interfaces of the security manager
0.2	1999-04-16	Modifications to the interfaces of the security manager: – Queries from L2CAP and other protocols harmonised – Only BD_ADDR used in query – Entity taking care of registration is implementation dependent. Registration moved to a separate section; interface to applications removed. – UI: set-up of trusted relationship included Security Policy for changed connection (section 2.1): wording changed to reflect that this includes client and server role. Section 3.1: – Pairing removed – registration can also be done by general management entity.

0.3	1999-04-27	– Remove parts for L2CAP connection hold after BB loss, because not supported by L2CAP any more: mainly changes in 3.5.2 and 3.5.3. – Flow chart changed according to phone meeting April 21st and included in document – Requirements for service security levels (requirement 3) corrected. Changes to distinguish between outgoing and incoming connections: – Default security level (in section 3.2.3) – Interface for registration: levels for both incoming and outgoing connections separately defined – Query to security manager: attribute for incoming/outgoing connection added Changes to make authentication mandatory in case authorisation is required: Statements in 3.2.1 and 3.2.3
0.5	1999-05-16	Security levels for registering multiplexing protocols added in section 3.6.5. Incorporate the changes agreed upon at the interoperability face-to-face meeting in Tampere: – Trust levels of devices might be set individually for services or groups of services. – Key management functions outside of Bluetooth mentioned – Trust flag replaced by more generic wording.
0.51	1999-05-26	Added statement on encryption in 2.1
0.8	1999-06-25	Introduction completely rewritten Requirements/Design objectives => what does the architecture provide Major editorial changes Removed chapter on consequences for Bluetooth specs Added section 4.6 Interface to HCI / Link Manager Added parameter ConnectionHandle in - 4.2 Interface to L2CAP - 4.3 Interface to other multiplexing protocols because it is needed in section 4.6 for HCI commands

0.86	1999-07-02	Incorporated changes from Chatschik and Jon • Abstraction: user ⇒ ESCE • Statement on application level security in Section 2.4 • Unknown device is also untrusted (Section 3.2.2) • Requirements for transition from security mode 2 to 3 added • Explanation for outgoing connections • Section 3.3.5.1 removed • Section 4.4: UI ⇒ ESCE and statements on calling directions
1.0	1999-07-13	Include PIN request to ESCE Terminology reference to GAP Replace initialization with bonding Editorial changes

Contributors

Paul Moran	3COM
Patric Lind	Ericsson
Patrik Olsson	Ericsson
Johannes Elg	Ericsson
Chatschik Bisdikian	IBM
Amal Shaheen	IBM
Jon Inouye	Intel
Robert Hunter	Intel
Brian Redding	Motorola
Stephane Bouet	Nokia
Thomas Müller (Owner)	Nokia
Martin Roter	Nokia

Disclaimer and copyright notice

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.