

ISO/IEC TR 16166:2010-08 (E)

Information technology - Telecommunications and information exchange between systems - Next Generation Corporate Networks (NGCN) - Security of session-based communications

| Contents | | Page |
|--------------------|---|-------------|
| Foreword | | v |
| Introduction | | vi |
| 1 | Scope | 1 |
| 2 | References | 1 |
| 3 | Terms and definitions | 3 |
| 3.1 | External definitions | 3 |
| 3.2 | Other definitions | 4 |
| 4 | Abbreviations | 4 |
| 5 | Background | 5 |
| 6 | General principles | 5 |
| 6.1 | Threats and counter-measures | 5 |
| 6.2 | Threats to session level security | 6 |
| 6.3 | Authorisation | 7 |
| 6.4 | Security and mobile users | 8 |
| 6.5 | Security and NGN | 8 |
| 6.6 | Security and software status | 8 |
| 6.7 | Call recording and audit | 8 |
| 7 | Signalling security | 8 |
| 7.1 | Security of access to session level services | 9 |
| 7.2 | Securing a SIP signalling hop | 9 |
| 7.2.1 | TLS for securing SIP signalling | 10 |
| 7.2.2 | IPsec for security SIP signalling | 10 |
| 7.2.3 | The role of SIP digest authentication | 10 |
| 7.3 | Ensuring that all SIP signalling hops are secured | 11 |
| 7.4 | End-to-end signalling security | 12 |
| 7.4.1 | End-to-end security using S/MIME | 12 |
| 7.4.2 | Near end-to-end security using SIP Identity | 13 |
| 7.5 | Authenticated identity delivery | 13 |
| 7.5.1 | P-Asserted-Identity (PAI) | 14 |
| 7.5.2 | Authenticated Identity Body (AIB) | 14 |
| 7.5.3 | SIP Identity | 14 |
| 7.5.4 | Authenticated response identity | 15 |
| 7.6 | NGN considerations | 16 |
| 7.7 | Public Switched Telephony Network (PSTN) interworking | 17 |
| 8 | Media security | 18 |
| 8.1 | SRTP | 18 |
| 8.2 | Key management for SRTP | 18 |
| 8.2.1 | Key management on the signalling path | 18 |
| 8.2.2 | Key management on the media path | 20 |
| 8.3 | Authentication | 21 |

| | | |
|-------|---|----|
| 8.3.1 | Authentication with key management on the signalling path | 21 |
| 8.3.2 | Authentication with DTLS-SRTP | 22 |
| 8.3.3 | Authentication with ZRTP | 22 |
| 8.4 | Media recording | 22 |
| 8.5 | NGN considerations | 23 |
| 9 | Use of certificates | 24 |
| 10 | User interface considerations | 24 |
| 11 | Summary of requirements, recommendations and standardisation gaps | 25 |
| 11.1 | Requirements on NGNs | 25 |
| 11.2 | Recommendations on enterprise networks | 25 |
| 11.3 | Standardisation gaps | 26 |