

Torsten Becker, Bernd Dusemund, Lutz Gollan, Thomas Engel, Christoph Meinel

## Trust Centre: Infrastructure, Specifications and Standards

### Content

<b>1 Infrastructure of a Trust Centre</b> .....	<b>1</b>
1.1 Registration .....	1
1.2 Key Generation .....	2
1.3 Personalisation and Key Delivery.....	4
1.4 Certificates .....	5
1.5 Directory Service.....	6
1.6 Time Stamp Service.....	7
1.7 Architectural Requirements.....	9
1.8 Documentation and Archiving .....	11
1.9 Business Continuity.....	12
1.10 Backup .....	15
1.11 Cross-Certification.....	15
<b>2 Technical Requirements .....</b>	<b>17</b>
2.1 Standardisation Committees .....	17
2.2 Evaluation .....	18
2.3 Standards and Specifications.....	21
2.3.1 Smart Cards .....	21
2.3.2 Signature Algorithms .....	23
2.3.3 Certificates .....	25
2.3.4 Names.....	28
2.3.5 Interchange Formats.....	28
2.3.6 Directory Service .....	29
2.3.7 Revocation Lists .....	30
2.3.8 Time Stamp Service .....	32
2.3.9 Profiles for a Security Infrastructure.....	32
<b>References .....</b>	<b>34</b>
<b>Glossary .....</b>	<b>40</b>