

ISO/IEC 29167-11:2023-02 (E)

Information technology - Automatic identification and data capture techniques - Part 11: Crypto suite PRESENT-80 security services for air interface communications

Contents		Page
Foreword		v
Introduction		vi
1 Scope		1
2 Normative references		1
3 Terms, definitions, symbols and abbreviated terms		1
3.1 Terms and definitions		1
3.2 Symbols		2
3.3 Abbreviated terms		3
4 Conformance		3
4.1 Air interface protocol specific information		3
4.2 Interrogator conformance and requirements		3
4.3 Tag conformance and requirements		3
5 Introduction of the PRESENT-80 cryptographic suite		4
6 Parameter and variable definitions		4
7 Crypto suite state diagram		4
8 Initialization and resetting		5
9 Authentication		5
9.1 Introduction		5
9.2 Message and response formatting		5
9.3 Tag authentication: AuthMethod "00"		6
9.3.1 General		6
9.3.2 TAM1 message		6
9.3.3 Intermediate Tag processing		7
9.3.4 TAM1 response		8
9.3.5 Final Interrogator processing		8
9.4 Interrogator authentication: AuthMethod "01"		9
9.4.1 General		9
9.4.2 IAM1 message		9
9.4.3 Intermediate Tag processing #1		9
9.4.4 IAM1 response		10
9.4.5 Intermediate Interrogator processing		10
9.4.6 IAM2 message		10
9.4.7 Intermediate Tag processing #2		10
9.4.8 IAM2 response		11
9.4.9 Final Interrogator processing		11
9.5 Mutual authentication: AuthMethod "10"		11
9.5.1 General		11
9.5.2 MAM1 message		12
9.5.3 Intermediate Tag processing #1		12
9.5.4 MAM1 response		12
9.5.5 Intermediate Interrogator processing		13
9.5.6 MAM2 message		13
9.5.7 Intermediate Tag processing #2		13
9.5.8 MAM2 response		14
9.5.9 Final Interrogator processing		14
10 Communication		14

11	Key table and Key update	14
Annex A	(normative) Crypto suite state transition table	15
Annex B	(normative) Errors and error handling	16
Annex C	(informative) Description of PRESENT	17
Annex D	(informative) Test vectors	22
Annex E	(normative) Protocol specific information	24
Bibliography		27