RFID Privacy Capability Statement for UHF interrogators

Product details for the interrogators

Manufacturer	
Product commercial reference	
Product type reference (if different from the commercial reference)	
Form completed by (company, if different from the manufacturer)	
Form completed by (person)	
Complies with standard (tick relevant standards)	**Complies with: ✓ box**
ISO/IEC 18000-63:2013	
ISO/IEC 18000-6: 2010 Type C	
ISO/IEC 18000-6:2004/ Amd 1:2006 Type C	
GS1 EPC UHF Air Interface Protocol Standard "Gen2v2"	
GS1 EPC UHF Class 1 Gen 2 Standard v. 1.2.0	
GS1 EPC UHF Class 1 Gen 2 Standard v. 1.1.0	
GS1 EPC UHF Class 1 Gen 2 Standard v. 1.0.9	
Frequency range	MHz to MHz
RFID commands supported by the interrogator (tick relevant commands)	**Supported: ✓ box**
Select — Command code: (A)h	
Req_RN — Command code: (C1)h	
Read — Command code: (C2)h	
Write — Command code: (C3)h	
Kill — Command code: (C4)h	
Lock — Command code: (C5)h	
Access — Command code: (C6)h	
BlockWrite — Command code: (C7)h	
BlockErase — Command code: (C8)h	
BlockPermalock — Command code: (C9)h	
ReadBuffer — Command code: (D2)h	
FileOpen — Command code: (D3)h	
Challenge — Command code: (D4)h	
Authenticate — Command code: (D5)h	
SecureComm — Command code: (D6)h	
AuthComm — Command code: (D7)h	
18000-63 Handle Sensor — Command code: (D9)h	
Untraceable — Command code: (E200)h	
FileList — Command code: (E201)h	
KeyUpdate — Command code: (E202)h	
TagPrivilege — Command code: (E203)h	
FilePrivilege — Command code: (E204)h	
FileSetup — Command code: (E205)h	

Additional proprietary or custom commands supported by the interrogator. Please list below	

Communication interface to the application	
Wired (define)	
USB (version)	
Wireless (define protocol)	

Privacy capability features supported by the interrogators

Code	Privacy capability features supported by the standards	Supported: ✓ box
C-1	Password protection[A] (Access Command code (C6)h)	
C-4	Cryptographic protection (Authenticate command code (D5)h)	
C-5	Symmetric-key cryptography (Authenticate command code (D5)h)	
C-6	Public-key cryptography (Authenticate command code (D5)h)	
C-9	Reduced Read Range (Command code (E200)h)	
C-12	Kill (Command code: (C4)h)	
C-16	Write (Lock) protection (Command code (C5)h)	
C-17	Temporary write Lock protection (Command code (C5)h)	
C-18	Permanent (or Perma) write Lock protection (Command code: (C9)h)	
C-19	Verification using a password (Command code: (C6)h)	
C-26	Verification using the unique Tag ID[B] (Command code: (C2)h of MB10)	
C-50	Hide TID (Command code (E200)h)	
C-51	Hide EPC or UII serial number (Command code (E200)h)	
C-52	Hide the entire User Memory (Command code (E200)h)	
C-53	Read/Write protection of specific User Memory file (Command code: (E204)h)	
Additional proprietary features supported by the interrogator. **Please list below.**		
With what kind of chip can your reader communicate? (**including all proprietary and custom commands**) Please list below (manufacturer and reference model).		
Manufacturer and model #1		
Manufacturer and model #2		
Manufacturer and model #3		
Manufacturer and model #4		
Manufacturer and model #5		
Manufacturer and model #6		
Manufacturer and model #7		
Manufacturer and model #8		
Manufacturer and model #9		
Manufacturer and model #10		
Can your reader handle any kind of chip's proprietary and custom command?	YES	NO
If yes, how is this achieved? Please explain.		

[A] In ISO/IEC 18000-6:2004 Am1: 2006 the password only protects the reserved memory bank. The cover coding does not help in protecting the consumer privacy as it only applies for protecting the password.

[B] For ISO/IEC 18000-6:2004 Am1: 2006, ISO/IEC 18000-63:2012 the TID may not be unique as this is not a requirement in the standard, however, most product vendors provide serialisation.