



Hardware for secure remote communication: market research

Hendrik Derre

Market Research

Industrial VPN Routers

- 10 leading Brands
- 26 unique devices

Goal:

- See what technologies are used for industrial equipment
- Provide information and advise what to use



Market Research

- Parameters

- Number of connections
- Transmission speed
- Number of VPN connections
- VPN network protocol
- Encryption
- Authentication
- Certificates
- Hashing algorithms

	Transmission Speed		#VPN connections	VPN Networking Protocol	Encryption	Authentication	
RS4000 TX/TX VPN	2	10/100	2	IPSec	DES, 3DES, AES-128/192/256	PSK, PKI	X.509v3
GUARD RS4000 TX/TX VPN	2	10/100	10 (250)	IPSec	DES, 3DES, AES-128/192/256	PSK, PKI	X.509v3 MD5, SHA
GUARD GT/GT VPN	2*	10/100/1000	10 (250)	IPSec	DES, 3DES, AES-128/192/256	PSK, PKI	X.509v3 MD5, SHA
*2 combo ports							
Siemens							
ALANCE S612	2	10/100/1000	128	IPSec	DES, 3DES, AES-128/192/256	PSK, PKI	X.509v3 MD5, SHA
ANCE S623	3	10/100/1000	128	IPSec	DES, 3DES, AES-128/192/256	PSK, PKI	X.509v3 MD5, SHA
S627-2M	3+2M*	10/100/1000	128	IPSec	DES, 3DES, AES-128/192/256	PSK, PKI	X.509v3 MD5
*Media Modules							
	8	10/100	10	IPSec (client server) L2TP(server) PPTP(client)	DES, 3DES, AES-128/192/256	PSK, PKI	
			50	IPSec (client server) L2TP(server) PPTP(client)	DES, 3DES, AES-128/192/256		

Market Research - report

Report available for download

- First preliminary results published on website
- User group input for additional parameters or devices possible
- Final version towards end of project
 - *Possible to input own research*

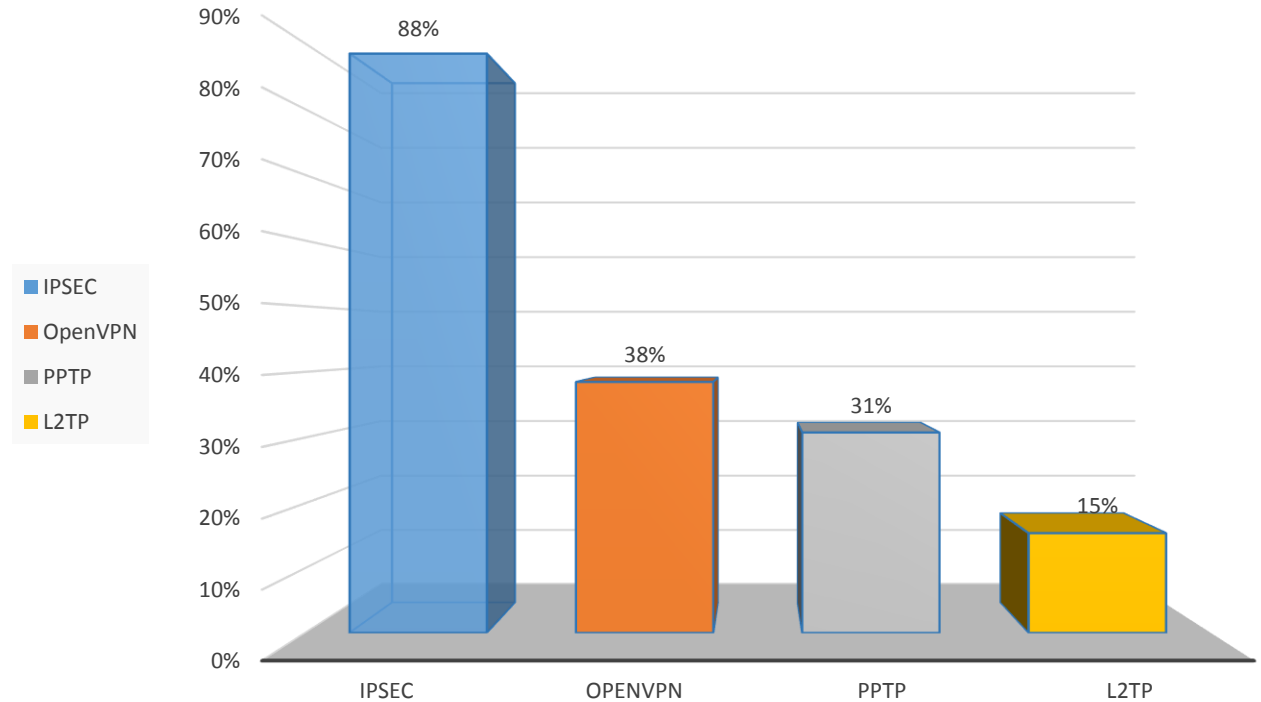
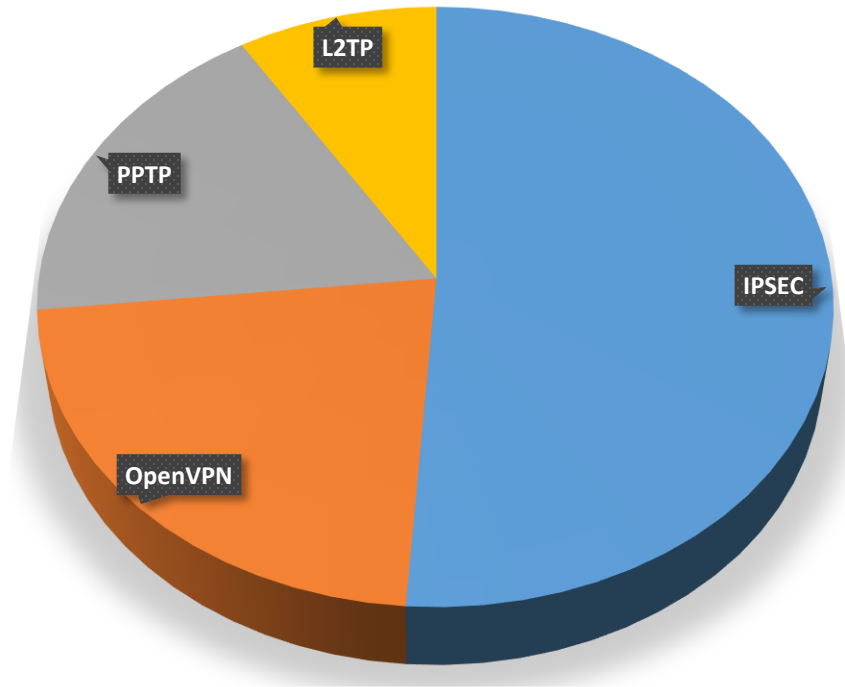
	Connections		VPN					
	#ports	Transmission Speed	#VPN connections	VPN Networking Protocol	Encryption	Authentication	Certificates	Hashing Algorithms
Phoenix Contact								
FL MGuard RS2000 TX/TX VPN	2	10/100	2	IPSec	DES, 3DES, AES-128/192/256	PSK, RSA	X.509v3	MD5, SHA-1
FL MGuard RS4000 TX/TX VPN	2	10/100	10 (250)	IPSec	DES, 3DES, AES-128/192/256	PSK, RSA	X.509v3	MD5, SHA-1
FL MGuard GT/GT VPN	2*	10/100/1000	10 (250)	IPSec	DES, 3DES, AES-128/192/256	PSK, RSA	X.509v3	MD5, SHA-1
*2 combo ports								
Siemens								
SCALANCE S612	2	10/100/1000	128	IPSec	DES, 3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA-1
SCALANCE S623	3	10/100/1000	128	IPSec	DES, 3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA-1
SCALANCE S627-2M	3+2M*	10/100/1000	128	IPSec	DES, 3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA-1
*Media Modules								
Moxa								
EDR-810 Series	8	10/100	10	IPSec (client server) L2TP(server) PPTP(client)	DES, 3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA
EDR-G902 Series	2*	10/100/1000	50	IPSec (client server) L2TP(server) PPTP(client)	DES, 3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA
EDR-G903 Series	3**	10/100/1000	100	IPSec (client server) L2TP(server) PPTP(client)	DES, 3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA
* 1 combo port ** 3 combo ports								
Hirschmann BELDEN								
EAGLE One Security Router	2	10/100		IPSec	3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA-1
EAGLE20-0400	4	10/100		IPSec	3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA-1
EAGLE30-0402	6	10/100/1000		IPSec	3DES, AES-128/192/256	Pre-shared key (PSK)	X.509v3	MD5, SHA-1
eWON								
eWON Coxy	4	10/100		OpenVPN 2.0 (SSL or HTTPS)	DES, 3DES, AES, BF	Public Key Infrastructure (PKI)	X.509v3	SHA-1
eWON Flexy	4*	10/100		OpenVPN 2.0 (SSL or HTTPS)	DES, 3DES, AES, BF	Public Key Infrastructure (PKI)	X.509v3	SHA-1
eWON CD	5	10/100		OpenVPN 2.0 (SSL or HTTPS)	DES, 3DES, AES, BF	Public Key Infrastructure (PKI)	X.509v3	SHA-1
* base station								
INSYS icom								
EBW Series	2	10/100		OpenVPN IPSec PPTP OpenVPN IPSec				
MuRoS Series	5	10/100						

Market Research - conclusions



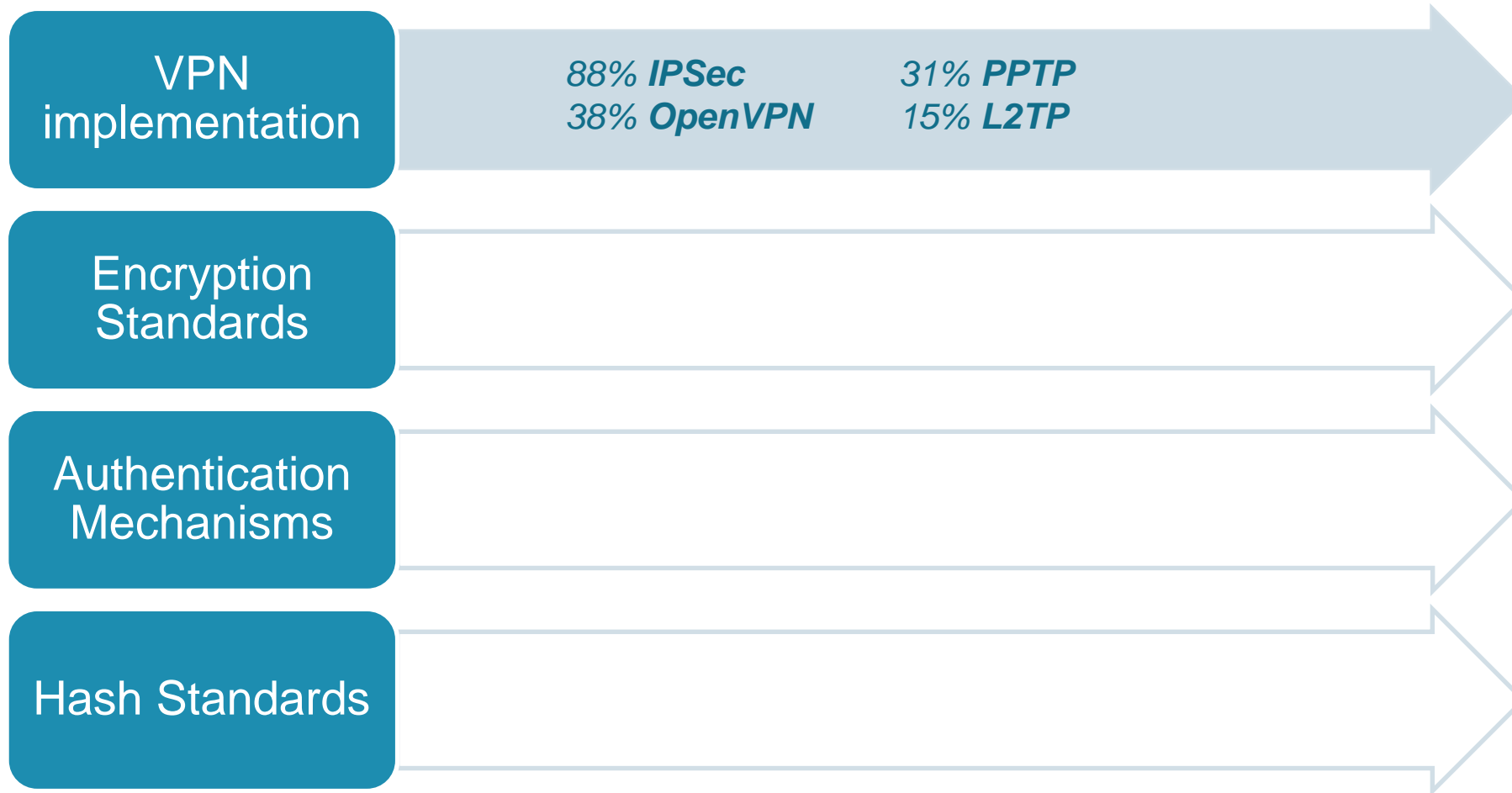
Market Research - conclusions

VPN Implementation



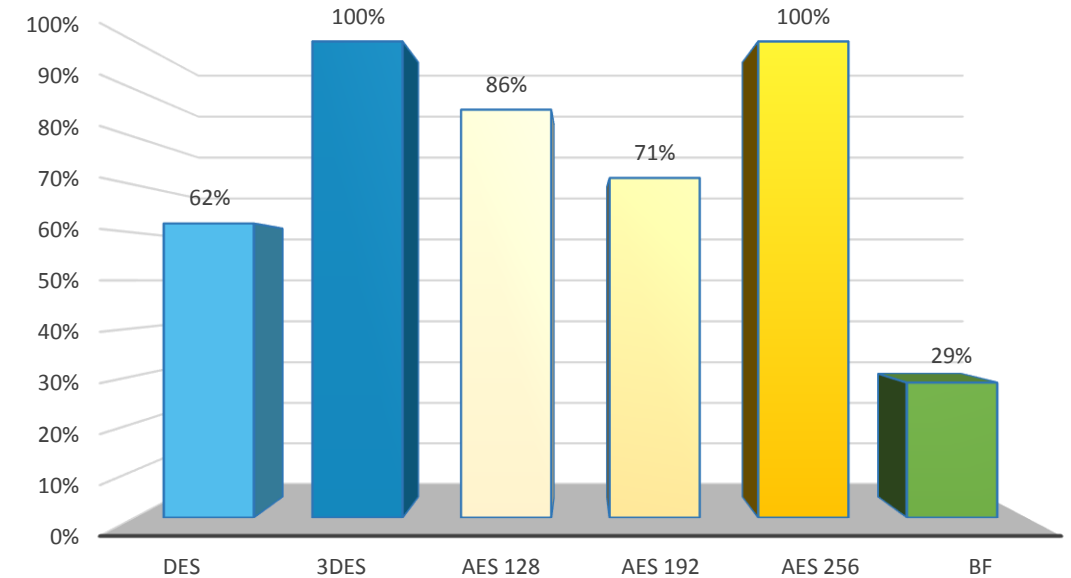
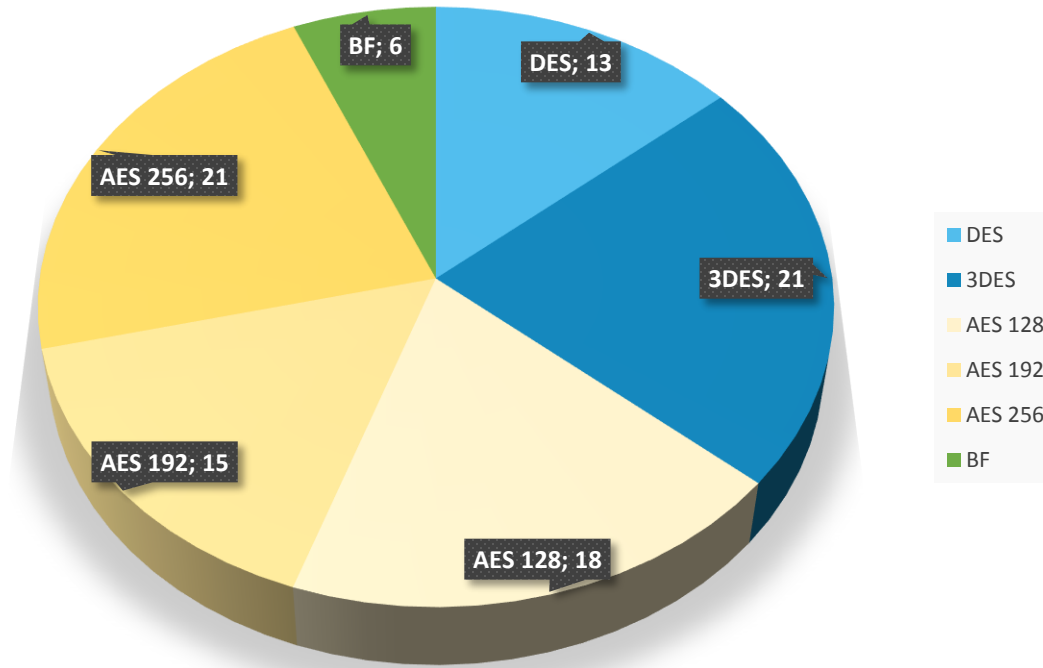
L2TP: Layer 2 Tunneling Protocol
PPTP: Point to Point Tunneling Protocol

Market Research - conclusions



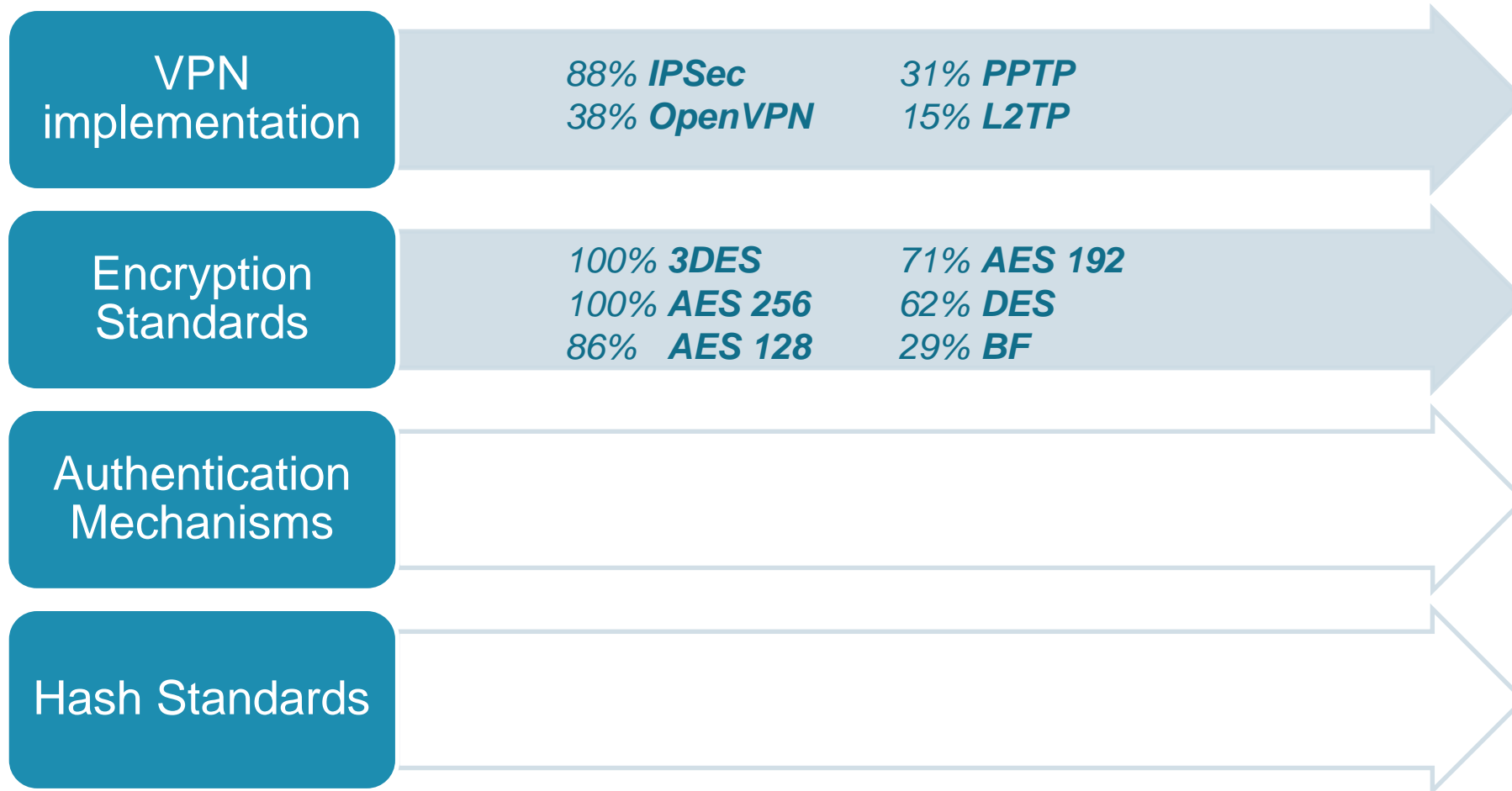
Market Research - conclusions

Encryption Standards



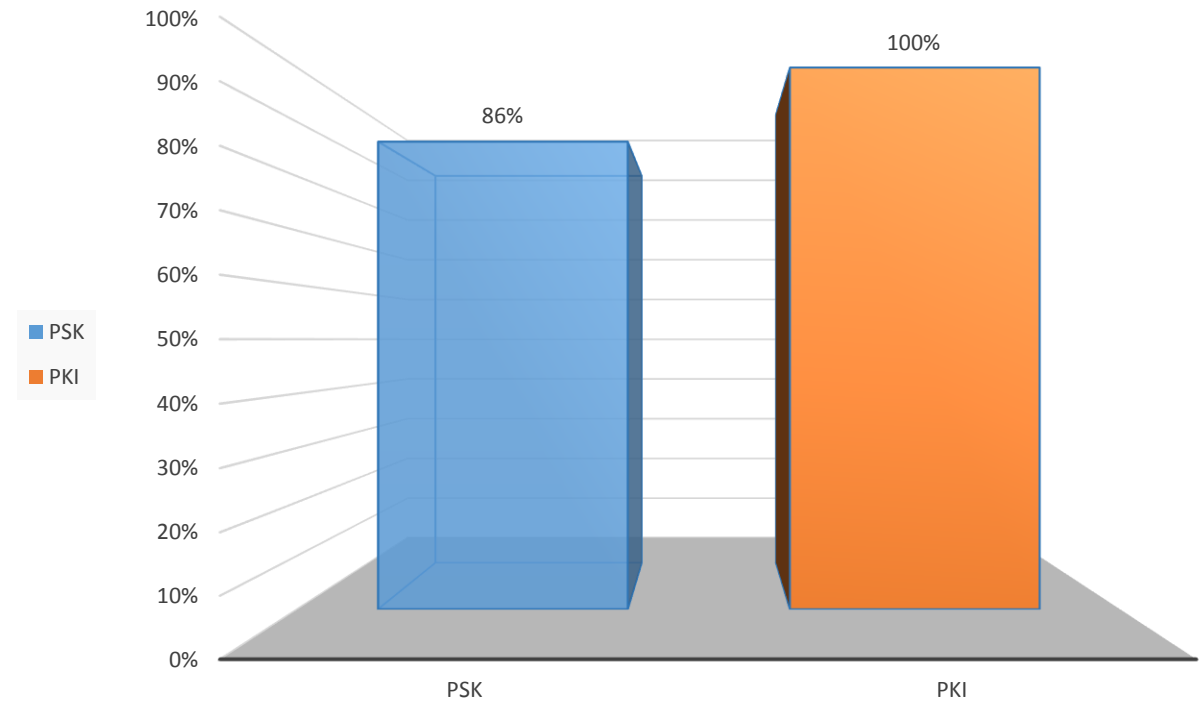
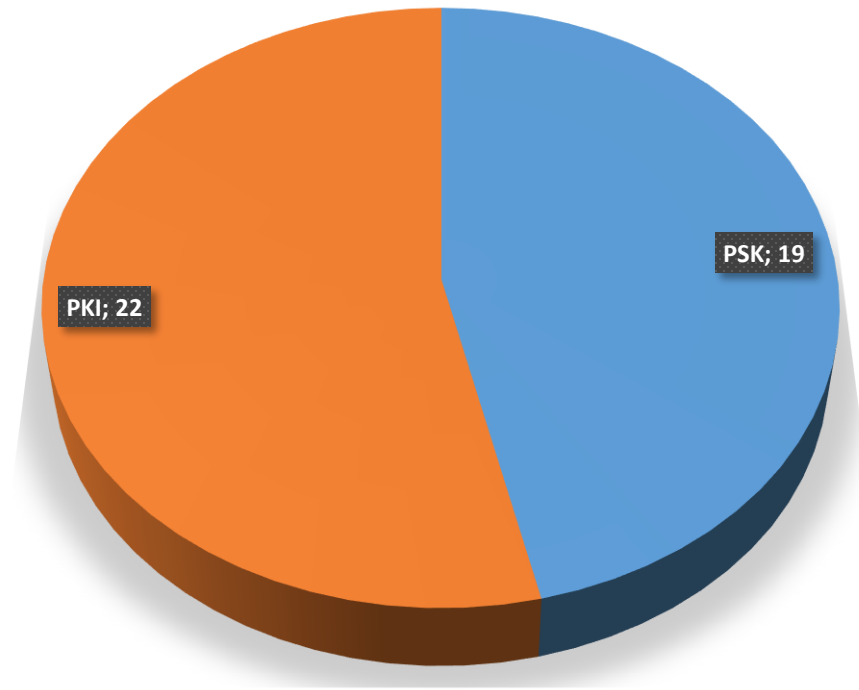
AES: Advanced Encryption Standard
DES: Data Encryption Standard
3DES: Triple Data Encryption Standard
BF: Blowfish

Market Research - conclusions



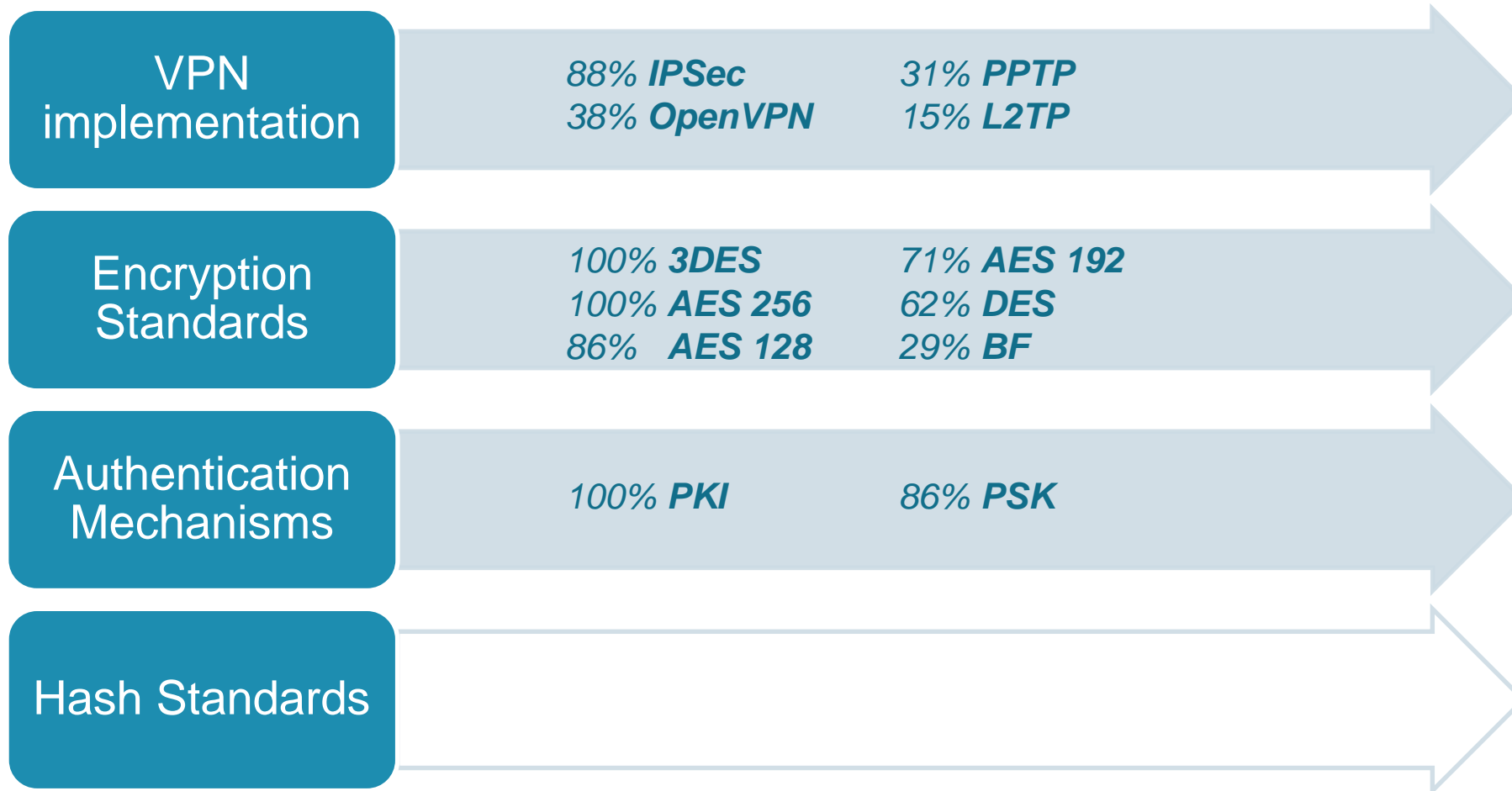
Market Research - conclusions

Authentication Mechanisms



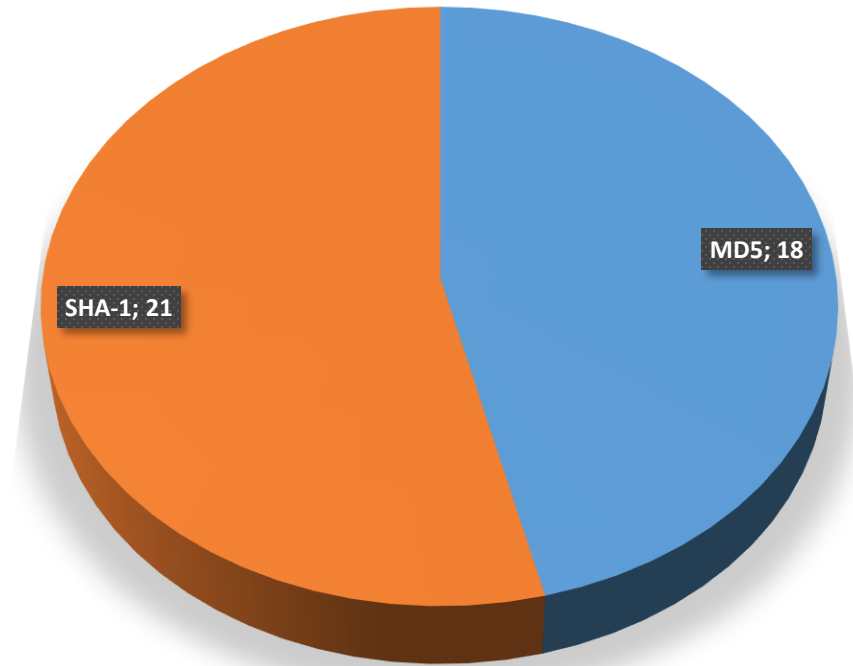
PKI: Public-key infrastructure
PSK: Pre-shared key

Market Research - conclusions

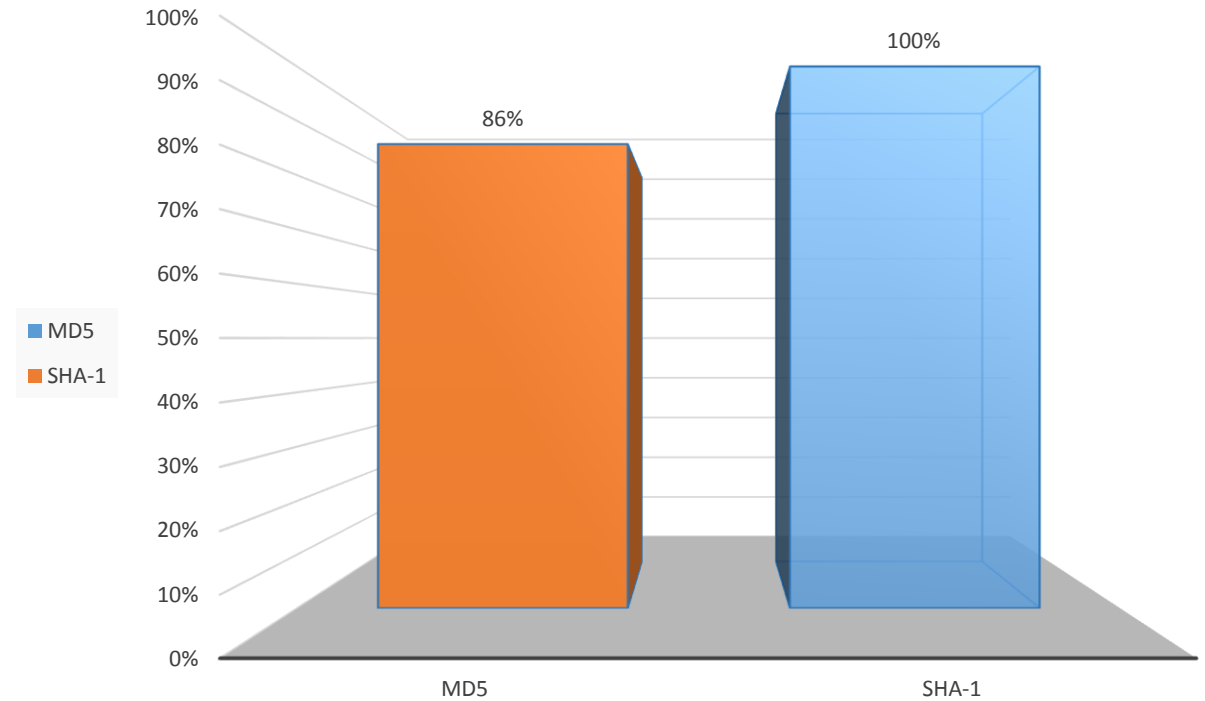


Market Research - conclusions

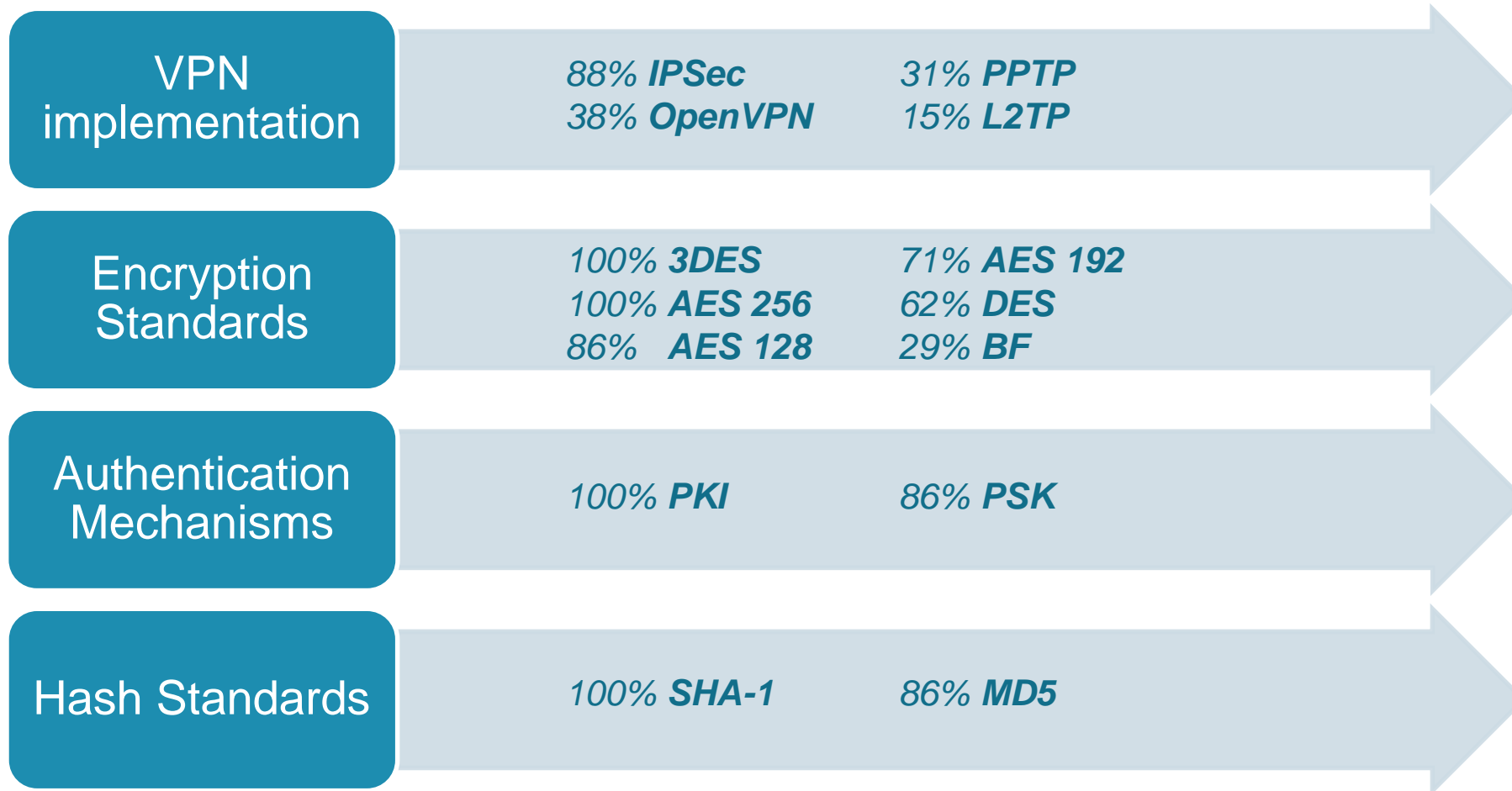
Hash Standards



MD5: Message-Digest Algorithm: 128bit hash value
SHA-1: Secure Hash Algorithm 1: 160bit hash value



Market Research - conclusions



Market Research - conclusions

- **From preliminary results some conclusions can be drawn**
 - VPN implementation: openVPN & IPSEC
 - Encryption: 3DES & AES256
 - Authentication: passwords (PSK) are still often used!
 - Difficult to manage
 - Danger of standard passwords

