Summary of strings to be passed as arguments to the different factories

In this document we present a table summarizing the different possible strings to be passed to each Factory in order to create an instance of an algorithm we request by the corresponding factory.

The general usage is as follows:

```
Algorithm myAlg = (Casting may be needed) [Algorithm]Factory.getInstance().getObject([relevant string]);
```

A specific example would be:

```
CryptographicHash hashH = CryptographicHashFactory.getInstance().getObject(“SHA1”, “BC”);
```

Or

```
CryptographicHash hashH = CryptographicHashFactory.getInstance().getObject(“SHA1”, “CryptoPP”);
```

Or

```
CryptographicHash hashH = CryptographicHashFactory.getInstance().getObject(“SHA1”);
```

In all cases the factory can be called without passing the provider argument therefore relying on SCAPI’s choice of the best provider implementation. Of course you must always pass the name of the algorithm you request.

Family	Algorithm	Parameters	String	Providers	Factory	Concrete Example
Cryptographic Hash	SHA-1	-	SHA-1	BC, CryptoPP	CryptographicHashFactory	…getObject(“SHA-1”) …getObject(“SHA-1”, “BC”)
	SHA-224	-	SHA-224	BC, CryptoPP		…getObject(“SHA-224”) …getObject(“SHA-224”, “CryptoPP”)
	SHA-256	-	SHA-256	BC, CryptoPP		
	SHA-384	-	SHA-384	BC, CryptoPP		
	SHA-512	-	SHA-512	BC, CryptoPP		
DlogGroup	DlogECFp	-	DlogECFp	BC, Miracl	DlogGroup Factory	…getObject("DlogECFp", “BC”);
		Name of curve	DlogECFp(nameOfCurve)			…getObject("DlogECFp(P-224)", “Miracl”);
	DlogECF2m	-	DlogECF2m	BC, Miracl		…getObject("DlogECF2m", “Miracl”);
		Name of curve	DlogECF2m(nameOfCurve)			…getObject("DlogECF2m(B-233)", “BC”);
	DlogZpSafePrime	-	DlogZpSafePrime	CryptoPP		…getObject(“DlogZpSafePrime”);
		num of bits for p	DlogZpSafePrime(numOfBitsForP)			…getObject(“DlogZpSafePrime(1024)”);
		q,g,p	DlogZpSafePrime(valueOfQ, valueOfG, valueOfP)			Too long to write it here. See below *
KeyDerivation Function	KdfISO18033	-	KdfISO18033			…getObject(“KdfISO18033”);
		Name of CryptographicHash	KdfISO18033(SHA-1)	BC	KdfFactory	…getObject(“KdfISO18033(SHA-1”);
			KdfISO18033(SHA-224)			
			KdfISO18033(SHA-256)			
			KdfISO18033(SHA-384)			
			KdfISO18033(SHA-512)			
	HKDF	-	HKDF	Scapi	KdfFactory	…getObject("HKDF”);
		Hmac	HKDF(Hmac(SHA-1)			
			HKDF(Hmac(SHA-224)			
			HKDF(Hmac(SHA-256)			…getObject("HKDF(HMac(SHA-256)”);
			HKDF(Hmac(SHA-384)			
			HKDF(Hmac(SHA-			

			512)			
PaddingScheme	BitPadding	-	BitPadding	Scapi	PaddingFactory	…getObject(“BitPadding”);
	NoPadding	-	NoPadding			…getObject(“NoPadding”);
	PKCS7Padding	-	PKCS7Padding			…getObject(“PKCS7Padding”);

Prf	Hmac	-	Hmac	BC	PrfFactory	..getObject(“Hmac”, “BC”);
		Name of CryptographicHash	Hmac(SHA-1)			
			Hmac(SHA-224)			
			Hmac(SHA-256)			…getObject(“Hmac(SHA-256)”);
			Hmac(SHA-384)			
			Hmac(SHA-512)			
	IteratedPrfVarying	-	IteratedPrfVarying	Scapi		…getObject(“IteratedPrfVarying(Hmac(SHA-256))”);
			IteratedPrfVarying (Hmac)			
			IteratedPrfVarying (Hmac(SHA-1))			
			IteratedPrfVarying (Hmac(SHA-224))			
		Name of PrfVaryingInput Length	IteratedPrfVarying (Hmac(SHA-256))			
			IteratedPrfVarying(Hmac(SHA-384))			
			IteratedPrfVarying (Hmac(SHA-512))			
	PrfVaryingFromPrfVaryingInput	-	PrfVaryingFromPrfVaryingInput	Scapi		
		Name of PrfVaryingInput Length	PrfVaryingFromPrfVaryingInput (Hmac)			
			PrfVaryingFromPrfVaryingInput (Hmac(SHA-1))			
			PrfVaryingFromPrfVaryingInput (Hmac(SHA-			

			224))			
			PrfVaryingFromPrfVaryingInput (Hmac(SHA-256))			
			PrfVaryingFromPrfVaryingInput (Hmac(SHA-384))			
			PrfVaryingFromPrfVaryingInput (Hmac(SHA-512))			
	PrpFromPrfVarying					…getObject(“PrpFromPrfVarying”)
	PrpFromPrfVarying	-	PrpFromPrfVarying	Scapi		…getObject(“PrpFromPrfVarying (IteratedPrfVarying(HMac(SHA-224)))”);
		Name of PrfVaryingIOLength	PrpFromPrfVarying (IteratedPrfVarying(HMac(SHA-224)))			…getObject(“PrpFromPrfVarying (IteratedPrfVarying(HMac(SHA-224)))”); …getObject(“LubyRackoffPrpFromPrfVarying”)
			Same as above with different CryptographicHash functions			
	LubyRackoffPrpFromPrfVarying	-	LubyRackoffPrpFromPrfVarying	Scapi		…getObject(“LubyRackoffPrpFromPrfVarying (IteratedPrfVarying(HMac(SHA-224)))”);
		Name of PrfVaryingIOLength	LubyRackoffPrpFromPrfVarying (IteratedPrfVarying(HMac(SHA-224)))			…getObject(“AES”);
	AES	-	AES	BC		…getObject(“TripleDES”);
	TripleDES	-	TripleDES	BC		

Family	Algorithm	Parameters	String	Providers	Factory	Concrete Example
PseudorandomGenerator	RC4	-	RC4	BC	PrgFactory	…getObject(“RC4”);
TrapdoorPermutation	RSA		RSA	BC, CryptoPP	TrapdoorPermutationFactory	…getObject(“RSA”, “BC”);
		Name of SecureRandom algorithm	RSA([SecureRandomName])			…getObject(“RSA(SHA1PRNG)”, “CryptoPP”)
	Rabin	-	Rabin	CryptoPP		…getObject(“Rabin”);
UniversalHash	Evaluation Hash	-	EvaluationHash	Scapi	UniversalHashFactory	…getObject(“ EvaluationHash(BitPadding, SHA1PRNG)”);
		Name of padding scheme, Name of SecureRandom algorithm	EvaluationHash(BitPadding, SHA1PRNG)			

* Example of DlogZpSafePrime passing possible values of q, g, p for bit length of p 1024:

String q = new String(“835846008601677106140729745932016701201219333799443460395370465895569997804629010752781250629134530929429112872868679572326603804690505362320832125653370919560505838303093666596306152054061466373811804087730135201426541046408104478575765469345002559000480981588439746339107720604305433960830960577104247365 91”);

String g = new String(“2”);

String p = new String(167169201720335421228145949186403340240243866759888692079074093179113999560925802150556250125826906185885822574573735914465320760938101072464166425130674183912101167660618733319261230410812293274762360817546027040285308209281620895715153093869000511800096196317687949267821544120861086792166192115420849473183”);

DlogZpSafePrime myDlog = DlogGroupFactory.getInstance().getObject(“DlogZpSafePrime(“ + q + “,” + g + “,” + p “)”);