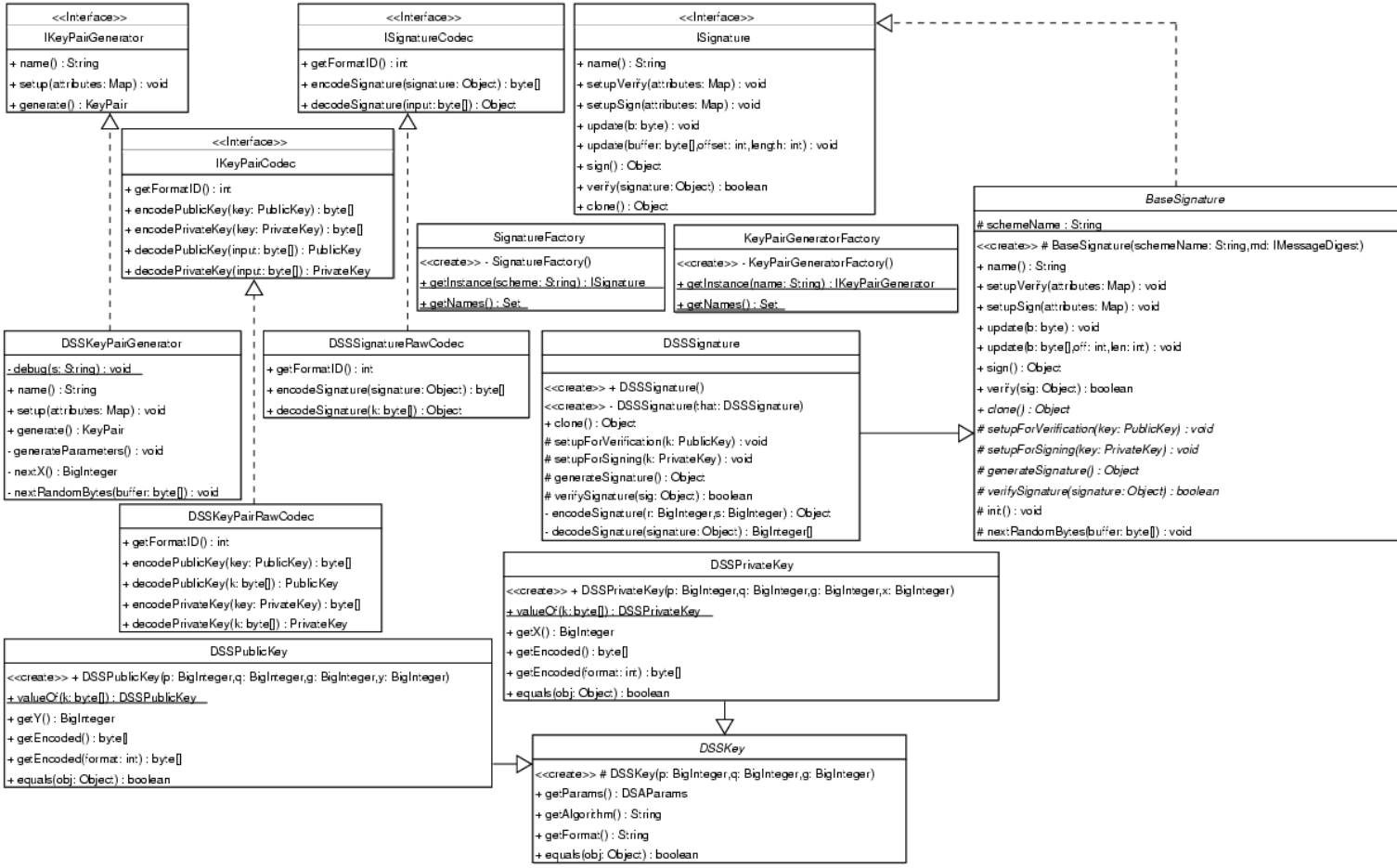
<<Interface>>
IKeyPairGenerator
+ name() : String
+ setup(attributes: Map) : void
+ generate() : KeyPair
<<Interface>>
ISignatureCodec
+ getFormatID() : int
+ encodeSignature(signature: Object) : byte[]
+ decodeSignature(input: byte[]) : Object
<<Interface>>
ISignature
+ name() : String
+ setupVerify(attributes: Map) : void
+ setupSign(attributes: Map) : void
+ update(b: byte) : void
+ update(buffer: byte[],offset: int,length: int) : void
+ sign() : Object
+ verify(signature: Object) : boolean
+ clone() : Object
<<Interface>>
IKeyPairCodec
+ getFormatID() : int
+ encodePublicKey(key: PublicKey) : byte[]
+ encodePrivateKey(key: PrivateKey) : byte[]
+ decodePublicKey(input: byte[]) : PublicKey
+ decodePrivateKey(input: byte[]) : PrivateKey
SignatureFactory
<<create>> - SignatureFactory()
+ getInstance(scheme: String) : ISignature
+ getNames() : Set
KeyPairGeneratorFactory
<<create>> - KeyPairGeneratorFactory()
+ getInstance(name: String) : IKeyPairGenerator
+ getNames() : Set
BaseSignature
schemeName : String
<<create>> # BaseSignature(schemeName: String,md: IMessageDigest)
+ name() : String
+ setupVerify(attributes: Map) : void
+ setupSign(attributes: Map) : void
+ update(b: byte) : void
+ update(b: byte[],off: int,len: int) : void
+ sign() : Object
+ verify(sig: Object) : boolean
+ clone() : Object
# setupForVerification(key: PublicKey) : void
# setupForSigning(key: PrivateKey) : void
# generateSignature() : Object
# verifySignature(signature: Object) : boolean
# init() : void
# nextRandomBytes(buffer: byte[]) : void
DSSKeyPairGenerator
- debug(s: String) : void
+ name() : String
+ setup(attributes: Map) : void
+ generate() : KeyPair
- generateParameters() : void
- nextX() : BigInteger
- nextRandomBytes(buffer: byte[]) : void
DSSSignatureRawCodec
+ getFormatID() : int
+ encodeSignature(signature: Object) : byte[]
+ decodeSignature(k: byte[]) : Object
DSSSignature
<<create>> + DSSSignature()
<<create>> - DSSSignature(that: DSSSignature)
+ clone() : Object
# setupForVerification(k: PublicKey) : void
# setupForSigning(k: PrivateKey) : void
# generateSignature() : Object
# verifySignature(sig: Object) : boolean
- encodeSignature(r: BigInteger,s: BigInteger) : Object
- decodeSignature(signature: Object) : BigInteger[]
DSSKeyPairRawCodec
+ getFormatID() : int
+ encodePublicKey(key: PublicKey) : byte[]
+ decodePublicKey(k: byte[]) : PublicKey
+ encodePrivateKey(key: PrivateKey) : byte[]
+ decodePrivateKey(k: byte[]) : PrivateKey
DSSPrivateKey
<<create>> + DSSPrivateKey(p: BigInteger,q: BigInteger,g: BigInteger,x: BigInteger)
+ valueOf(k: byte[]) : DSSPrivateKey
+ getX() : BigInteger
+ getEncoded() : byte[]
+ getEncoded(format: int) : byte[]
+ equals(obj: Object) : boolean
DSSPublicKey
<<create>> + DSSPublicKey(p: BigInteger,q: BigInteger,g: BigInteger,y: BigInteger)
+ valueOf(k: byte[]) : DSSPublicKey
+ getY() : BigInteger
+ getEncoded() : byte[]
+ getEncoded(format: int) : byte[]
+ equals(obj: Object) : boolean
DSSKey
<<create>> # DSSKey(p: BigInteger,q: BigInteger,g: BigInteger)
+ getParams() : DSAParams
+ getAlgorithm() : String
+ getFormat() : String
+ equals(obj: Object) : boolean