成プロセスの各ステップで経済と学術の専門家の助言を求めること。責任規制官庁は、学界と経済界から提起された問題を解決に導き、決定を下す権限と義務を有する。

§13 について（ドキュメント）

1 項について

安全措置のドキュメント作成はデジタル署名法§13 および署名省令§15 による監察の実施のため必要である。その他の資料のドキュメント作成は、たとえば証明書偽造の疑いがあるとき必要である。それ以外に自動的にプロトコールデータ（例えば証明書発行機関の個人サインコード使用について）が作られるとき、そのドキュメントを作成するのは証明書発行機関の裁量に属する。

この最後の段の規定はドキュメント化されたデータが変造されないことを保証するのが目的であって、記録のサインには別のサインコードが必要である（デジタル署名法§4、5 項についての理由説明参照）。

2 項について

保存期間の計算は特に、民法§195 記載の規定の消滅時効期間（30 年）が重要でありうる署名法使用ケースでも、それに応じた保存期間が確保されるよう配慮したものである。この計算はまた証明書の許容有効期間をも考慮している。古い署名法が§18 に従い新しい署名法のよって長い期間「保存」される場合、消滅時効期間内では古い署名法チェックの可能性が保持できるようにする（例えば裁判所によって）。特定の分野（例えば医療）で、もっと長い保存期間が必要ならば、自己の証明書発行機関によってあるいは契約合意によってそれを確保しなければならない。

ドキュメント作成がデジタル形式で行われる場合（例えば証明書で）、「使える」とは「チェック可能」を含む。つまり、それに適したハード・ソフトウエアを備えなければならない。これに類した長い期間としては、例えば飛行機製造の「デジタルドキュメント」（50 年）、長期間にわたってデータを記入する電子土地台帳がある。

デジタル署名法§12、2 項の問合せ回答のドキュメントについては電気通信法§90 の場合と同じく 12 ヶ月の保存期間を定めている。

§14 について（営業停止）

1 項について

この規定は所轄官庁が 2〜4 項で義務づけされている、証明書発行機関営業停止の際の手続を監視できるようにするのが目的である。

ここに記した期間および 2 項の期間は通常の営業停止に適用される。倒産とか営業許可撤回・取消しの場合はもっと短い通知期間が必要なこともありうる。

2 項について

ある証明書発行機関が営業停止する場合、そのサインコード所持者には早めに知らせ、他の証明書発行機関ですぐに新しい証明書を取得できるようにする。所持する証明書が他の証明書発行機関に引き継がれる場合、サインコード所持者がそれを望まなければ、使用禁止措置をとることができる。

証明書発行機関が証明書引継ぎの他の証明書発行機関を見つけることができなかったため、証明書が証明書発行機関によって使用禁止される場合、サインコード所持者には現時点での使用禁止のプロセスについて教示すること。

3 項について

通知の形式上の要求は通知の偽造を防止するのが目的である。

4 項について

この規定は、デジタル署名法および署名省令で決められている証明書のチェック可能性を証明書発行機関が営業を停止したときにも確保するためのものである。

所轄官庁は引継ぎの場合、他の証明書発行機関に管理を委託することもできる。そのコストは引き渡す証明書発行機関が負担する（§2、1 項 No. 7 参照）。

§15 について（証明書発行機関の監察）

1 項について

この監察は必要な安全性を長期にわたって確保するのが目的である。「営業開始」とははじめて営業を行うことをのみ意味する。いつ変更は安全にとって重要なものになり、デジタル署名法§4、3 項 3 段による新たな検査（2 年毎の定期検査と並んで）と確認とが必要になるかについて疑問が生じた場合、証明書発行機関は所轄官庁と相談してクリアしなければならない。証明書発行機関は通常、受付事務所を方々に置いた分散構造であるが、デジタル署名法と署名省令の実施に関しては、本社と、それから抜取りで幾つかの受付事務所の作業、および受付事務所・本社間の連絡作業をチェックすれば十分である。

デジタル署名法§4、3 項 3 段に従い承認を受けた、デジタル署名法と署名省令の規定順守検査・確認のための機関は所轄官庁の「行政協力者」として作業を行う。これら機関の選択と承認とは専門的な観点に立ち、必要性に応じ、義務に従った自己の裁量で行う。 デジタル署名法§4、

3項3段に従った検査と確認との前提となるのは、行政・技術安全の分野で実績があることを証明し（実績照会先の提示）、1項に従って所轄官庁の監督のもとに、BSIの協力を得て有効な検査を行った経験を有することである。DIN EN 45000以下に従い検査と監督とは2つの互いに無関係な機関が実施する。検査・確認機関は所轄官庁による承認を必要とする。これには例えば、BSI設置法により情報技術の検査と情報技術安全の問題でのコンサルテーションを委託されている連邦情報技術安全局（BSI）（デジタル署名法§14、4項についての理由説明も参照）を承認された機関として使うことができが、他の検査・確認機関も対象となる。

2項について

1項の規定に従って広範囲な検査を行えば、あとは所轄官庁による、必要に応じた抜取の監察で十分であると考えられる。所轄官庁は義務に従った自己の裁量で監察の頻度と規模を決める。平均して年に1証明書発行機関当り1度の監察が適当である。監察には技術チェックも含めることができる。

§16について（技術コンポーネントへの要求）

この項目はデジタル署名法§14の技術コンポーネントへの安全性への要求を、技術イノベーションの余地を限定することなく、スペック化するのが目的である。従って要求は目標設定に限定される。

1項について

1段のコードの一回性の要求は入手可能なコードジェネレーターで満たすことができる。

2段のコードの秘密保持にはコードメモリーについて、（サインコード所持者自身によっても）読み取れないような技術コンポーネント（例えばチップカードあるいは大コンピューター用の特殊コンポーネント）を必要とする。サインコードは外部で作成して、チップカードに移すこともでき、最新のチップカードではチップカード自体の上で作成することができる。コードデータ媒体自体の上でのコード作成はその安全性を考えて将来標準とすべきであろう。

3段の（検査・確認された安全な状態に対する）安全技術上の変更というのは、技術的な変更のためコンポーネントの安全がもはや十分に与えられないときである。それは例えば外面的な破壊もしくは機能喪失によって発見可能となることがある。これによって、特に個人サインコードを探ろうとする安全技術上のマニピュレーションから技術コンポーネントの利用者を保護するのが目的である。

2項について

サイン技術は通常チップカードまたはそれに類した媒体（例えば PCMCIA カード）上で実施される。所有（カード）および知識（PIN またはパスワード）以外のサインコードの所持者への結びつきを達成するため、バイオメトリックな標識（例えば顔、自署、指紋）を用いることができる。

技術コンポーネントは、オプションで署名法の前、あるいは一定の数の署名法のあと、あるいはサイン技術を用いないときは一定の時間が経過してから、照合データをあらためてインプットしなければならないように形成することができる。利用環境によって、どの方式をとるかは、利用者の裁量に属する。

6 段により安全技術上の変更を発見できるようにして、特に個人サインコードもしくは照合データを探ろうとする安全技術上の変更から利用者を守るようにする。1 項についての理由説明も参照。

3 項について

署名法を作成する者は表示されたデータとサインされたデータ（例えばコールしたファイル）とが一致し、他のデータがサインに「押し込め」られないことを確かめなければならない（1 段）。署名法の検査では表示されたデータのサインが検査されたものであることを確かめなければならない。彼にとってまた、正確さのチェックは信頼できるものでなくてはならない（2 段）。

証明書のチェックの際（デジタル署名法§4、5 項 3 段および§5、1 項 2 段参照）、チェックする者にとっては、3 段に述べた事柄はその正確さに信頼がおけるものでなくてはならない。この規定は 4 項 2 段の証明書リスト作成のための技術コンポーネントの規定によって補足される。利用者は証明書の有効性を確かめる以下の可能性を有する：

・規制官庁の公開サインコードを使っての内部チェックにより、証明書が公式に許可された証明書発行機関によるものであり、証明書記載事項によりチェックすべき署名法作成の（記された、あるいは推定の）時点で証明書が有効であったことを確かめることができる。

・上に追加してオンラインで証明書発行機関の証明書リストにより、証明書がそこに記載されているか、署名法作成時に使用禁止されていなかったかのチェックを行うことができる。その代替として内部の最新の使用禁止リストに問い合わせることができる（§8、2 項および§9、3 項についての理由説明参照）。

・外国の証明書では上にさらに追加してオンラインで規制官庁の証明書リストにより、外国の根幹官庁の証明書がそこに記載されているかのチェックを行うことができる（§8、2 項 2 および 3 段参照）。

署名法はデジタル署名法§14、2項によりデジタルデータのみに関係し、その解釈（例えばテキスト、言語、音楽、ソフトウエア）には無関係である。しかしサインを作成あるいは検査する者は、必要に応じて（特にテキストで）サインすべき、あるいはサインされたデータの内容を「十分に」知ることができなければならない（4段）。特定の利用（例えばホームバンキング）では特殊なフォーマットと利用プログラムを用いることができる。
技術コンポーネントが営業目的で第三者に利用提供される場合、利用者がその真なることを利用開始の際自動的にチェックし（5段）、マニピュレーションされた技術コンポーネントによるデータの「押込み」を防止できるようにしなければならない。技術コンポーネントが真であることと安全状態とは例えば利用者のチップカードに対する自動認証操作によって確認することができる。
6段の安全技術上の変更を発見可能とすることは、個人的に利用される技術コンポーネントにも当てはまる。1項についての理由説明も参照。

4項について
この規定はデジタル署名法§14、3項を補足して、義務づけられている証明書リストを偽造証明書記載と不正変更（例えば使用禁止の証明書の取出し）から守り、呼出し可能でない証明書（例えば代行権についての付加証明書）を不正使用から守るのが目的である。アクセス権限のある人間による使用禁止の撤回（§9、3項参照）が技術的に防止できない場合、それは少なくとも発見されることなく可能であってはならない。
また、本物のリストを装うこと（「いわゆる仮装」）を防ぐため、問合せ回答の真なることの確実なチェックが可能でなくてはならない。
完全偽造をも防ぎ、それを少なくとも発見できるようにするため、問合せ回答は使用禁止についての記載事項と並んで、証明書が証明書公開リストに載っているかについての記載を含まなくてはならない。この手続において完全偽造のものを通用させようとする者は、偽造証明書を発行するだけでなく、それを同時にリストに入れ、監察があることを考えて証明書への偽造申請を記録させなければならないことになる（これはのちに偽造の証明になるであろう）。これによって証明書のチェックの際、利用者は少なくとも、証明書がリストに載っているか（イエス／ノー）、記された（サイン作成の）時点で使用禁止されていたか（イエス／ノー）を知ることができる。使用禁止された証明書については使用禁止の日付と時間に関する回答も必要である。
サインコード所持者の同意に基づき公開で呼び出し可能な状態におかれている証明書は法律で義務づけられているリストのほかに、法律規定の適用を受けない別のリストに載せることができる。これは使用禁止リストについても該当する（§9、3項についての理由説明参照）。証

明書自体はすでにその署名法によって偽造と発見されない変造に対し保護されている。証明書リストと変造リストも同じく署名法によって、発見できない変造から守ることができる。

5項について
1978年7月25日付時間法§1、1項（連邦法官報Ⅰp．1110、1262；1991年9月13日付法律により変更）により公務およびビジネスでは法定時間による日付と時刻とを用いる。「法定時間」は時間法§1、4項に中央ヨーロッパ時として定義され、夏時間を含む。
日付印作成のための技術コンポーネントはデジタル署名法§14には条文の形で述べられていないが、それが含まれていることはデジタル署名法§9とデジタル署名法§14から間接的に出てくる。

6項について
措置施行令では、デジタル署名法と署名省令の規定を満たすための実際的な方法を例を挙げて説明する。施行令はまた特に、統一規格（例えば所属のパラメーター証明書のフォーマットのついたアルゴリズムで）の一助とするのも目的である。デジタル署名法と署名省令の規定に矛盾しないかぎり、他のイノベーティブな方式のための余地を残すため、違った方法をとるのは差し支えない。決定的な意味をもつのは許可された専門機関によって法的整合性が確認されることである（デジタル署名法§14、4項および当説明§17、4項参照）。施行令は製作者のオリエンテーションと迅速な製品検査（§17参照）のためのもので、一般的な形で、デジタル署名法と署名省令の目標を達成するための、できるだけバラエティに富んだ技術方式を挙げている。その他の点では§12、2項の説明が準用される。

§17について（技術コンポーネントの検査）
1項について
検査されるべき技術コンポーネントと技術コンポーネントへの要求は§16に最終的な形で挙げられている。
挙げられている判断基準（英語の名称：「Infomation Technology Security Evaluation Criteria - ITSEC」）は情報技術コンポーネントとシステムの安全評価の国際的基準である（1995年4月7日付EC理事会提案95/144/ECも参照）。この基準は検査ないし評価段階（「E1」から「E6」までの段階がある）と安全目標を達成するために使われる機構の強さ（低、中、高に分ける）とを区別し、（連邦官報には公示されていないが、専門家には知られれいる）「情報技術システム安全ハンドブック」（英語の名称：「Infomation Technology Security Evaluation Manual - ITSEM」）によって補足される。将来実績のある新しい基準が出れば、署名省令を必要に応

じてそれに合わせる。
機構の強さが決定的要素となれば、署名省令はつねに「高」の段階を要求し、2項のアルゴリズムとそれに属するパラメーターについては、それに追加して明確な適正確認を要求する。機構に「高」の評点をつける前提条件はITSECに次のように記されている：「ある問題となっている機構の最低の強さが「高」と評価されるためには、それが極めて高度な専門知識、チャンス、技術手段を有する犯人によってのみ攻撃されるうるもので、そのような行為も通常は実行不可能であると判断されるものでなくてはならない。」
検査段階では、さまざまなリスクに従って、それぞれ違った要求が行われる。高い検査段階「E4」はサインコードの安全性と個人サインコードの秘密保持に使われる技術コンポーネント、および営業目的で第三者に利用提供される技術コンポーネントに対して要求される。この２つのケースでは隠れたエラー／マニピュレーションが重大な結果をもたらすことがある。しかしこれらは把握しやすい特殊コンポーネントであり、大掛かりな検査（例えば形式的な安全モデルを作成して）も適正な費用で実施可能である。そのほかの点では今日の標準検査段階「E2」（例えば機構のツール化のチェック、弱点分析、エラー追跡のテストを伴ったもの）で十分と思われ、現在の技術水準では適正な費用で実施可能である。署名法の検査には公開サインコードのみ使われるため、これはその技術コンポーネントにも当てはまる。
数学方式の適性確認、要求されている機構強度「高」およびリスクチェックによって
統一的な高い程度の最低安全性が達成される。これにさらに、3項3段による鑑定の形での抜取検査および疑問発生時チェックが加わる。検査段階の規定の最低高さは例えばエレクトロニックバンキングのための特殊コンポーネントでは自由競争によって越えることができる。
そこで、個々の技術コンポーネントに関しては以下のようになる：

－ コード作成のコンポーネント（チャージプロセスを含む）		E4 高
－ 個人サインコードメモリーと使用のためのコンポーネント		E4 高
－ 署名法作成のための他のコンポーネント、以下を含む ・ 照合データの把握と検査 ・ サインすべきデータの表示	E2	高
－ 署名法検査のためのコンポーネント、以下を含む ・サインされたデータの表示 ・証明書のチェック	E2	高

― 証明書チェック可能保持のためのコンポーネント	E2 高
― 日付印作成のためのコンポーネント	E2
―営業目的で第三者に利用提供される署名法の作成と検査のためのコンポーネント	E4 高

アルゴリズムとそれに属するパラメーターとは2項の規定を満たさなければならない。

2項について
使ったアルゴリズム（暗号方式）とそれに属するパラメーター（例えばコードの長さ）とは署名法安全の基礎をなすものである。従ってその適性は官庁、経済界、学界における暗号に関する専門知識を利用して確認し、適性確認は確実な表現ができる期間に限定する。6年の期間は専門家の計算では、アルゴリズムとそれに属するパラメーターの時間経過による安全値低下を考えても十分に見通しの利く期間である。十分な理由があれば、この期間を短縮あるいは延長することができる（「基準期間」）。（その「ノウハウ」の秘密保持のためもあって）、暗号作成・解読のためのアルゴリズムを評価するに際してBSIに課せられる慎重な態度は、署名法のため必要なアルゴリズムには適用されない。
サインされるべきデータの「ハッシュ」ではデータから1回性の「デジタル指紋」を取り、データ全体の代りにそれにサインする。ハッシュアルゴリズムは、異なるデータには同じハッシュ値は出ないことを確保しなければならない。
適性確認と毎年の評価更新のため設定される通常6年の最低期間は、適性確認の1年延長がないことが早期に決まれば、少なくとも1年の期間を新製品の導入のために予定しておく（§7、2項1段による新しい証明書通用の5年の期間はそれから始まるが、この期間は適性を有するアルゴリズムとパラメーターの使用によって完全にカバーされなくてはならない）。
新しい、適性を有する技術コンポーネントとの交替は通常漸次に行われるため、古い技術コンポーネントと新しい技術コンポーネントとを過渡期には併用することも必要であろう。
連邦情報安全局の協力に関しては§12、2項および§16、6項の説明が準用される。

3項について
1段は製品の適性について明確な説明を行うのが目的である。
続く規定は選択した構造（競合民営機関）の範囲内で、技術コンポーネントの統一的に高い安全性を確保するのが目的である。

3 段の鑑定では所轄官庁は、検査あるいは確認が連邦情報技術安全局自身によってなされたものでない限り、その協力を求めることができる。
技術コンポーネントの承認された機関の検査あるいは確認が正しくなかったことが判明すれば、所轄官庁は承認を取り消すことができる。
ある技術コンポーネントの確認の無効が宣言されれば（5 段）、それを 4 項により公示すること。そのほか所轄官庁は、サインコード作成のための技術コンポーネントもしくは個人サインコードのメモリーと使用のための技術コンポーネントの無効が宣言されれば、デジタル署名法§13、5 項 2 段の前提のもとで証明書の使用禁止をも指示することができる。証明書発行機関は証明書発行の際いずれにしても無効宣言された技術コンポーネントが使われないことを確保しなければならない（§5、1 項参照）。

4 項について
デジタル署名法§14、4 項によって承認された機関とこれら機関の確認を有する技術コンポーネントとは、必要に応じてだれもがそれを基準にすることができるよう公示すること。
デジタル署名法§14、4 項によって承認された機関は官庁の「行政協力者」として働く。デジタル署名法§14、4 項による技術コンポーネントの法的整合性を確認することが許される、複数の民営（安全証明書発行）機関を承認すること。

§18 について（新しい署名法）
署名法に使われるアルゴリズムとそれに属するパラメーターおよびそれによって作成される署名法が新しい科学的知識あるいは技術的進歩（例えばコンピューターが早くなる）の結果安全値を失えば、 アルゴリズムとそれに属するパラメーターの適性の期間が過ぎる前に、（新しい技術コンポーネントの）新しい署名法が必要となる。新しいサイン作成のため新しい技術コンポーネントの使用は、証明書発行機関がサインコード証明書の発行前に技術コンポーネントの適性を確認することと（§5、1 項参照）、証明書の有効期間は適性の期間を越えない(§7、2 項参照)ことによって確保される。
新しい署名法がのちの時点で（前の署名法の安全値がすでに減少して偽造が可能になってから）付けられ、遡及日付となるのを防ぐため、それには日付印が必要である。
のちの偽造の可能性を考慮して前の署名法を否定できないよう、それは新しい署名法に含ませ、「保存」しなければならない。ここでは任意の数のサインされたデータについて 1 つの（包括する）新しい署名法で十分であり、それは任意の人物（例えばアーヒヴァー）がつけることができる。
現在の署名法について、アルゴリズムとそれに属するパラメーターの適性期間経過後に§17、2

項に従って新しい署名法が付けられない場合、法定の安全性は失うが、それとは別に長期間高い安全値を保持することはありうる。しかしその評価が問題になれば、裁判所と専門家に委ねる。

§19 について（発効）

署名省令は 1997 年 11 月 1 日、つまりデジタル署名法にあまり遅れないよう発効させる。デジタル署名法によって予定されている§12、2 項および§16、6 項による措置施行令も同じく遅れないよう公示される。